



Proposta de solução de videovigilância para locais remotos

JAIME RAFAEL PINTO LOPES

Outubro de 2015

Proposta de solução de videovigilância para locais remotos

Jaime Rafael Pinto Lopes

**Dissertação para obtenção do Grau de Mestre em
Engenharia Informática, Área de Especialização em
Sistemas Gráficos e Multimédia**

Orientador: Professor Doutor António Vieira de Castro

Júri:

Presidente:

[Nome do Presidente, Categoria, Escola]

Vogais:

[Nome do Vogal1, Categoria, Escola]

[Nome do Vogal2, Categoria, Escola] (até 4 vogais)

Porto, Outubro de 2015

Agradeço do fundo do coração aos meus pais e irmãs, que me incentivaram a nunca desistir.

Á minha filha Cátia Lopes com muito amor e carinho, a quem devo muitas horas. Este trabalho foi realizado a pensar em ti.

“Hoje melhor do que ontem, amanhã melhor do que hoje!”

Resumo

Desde tempos remotos que homens faziam a vigilância de bens e mercadorias e mais recentemente também de pessoas com o intuito de dissuadir roubos, atos de vandalismo e de violência. Nos últimos anos, com a evolução das novas tecnologias verificou-se a sua adoção para auxílio da vigilância. Os atos de terrorismo que têm acontecido um pouco por todo o mundo trouxeram um clima de insegurança à população mundial. Este fenómeno, juntamente com o elevado número de roubos e atos de violência levou à expansão de utilização dos meios de videovigilância de forma a dissuadir estes tipos de crime podendo mesmo, nalguns casos servir como prova para punir os autores dos mesmos.

Em Portugal tem-se verificado uma escalada de crimes nas zonas mais rurais não só de bens como as alfaías agrícolas mas também de frutos e mesmo de animais. Estes crimes predominam em locais rurais, relativamente distantes das povoações e em locais onde não existem (ou são praticamente inexistentes) infraestruturas necessárias para implementar meios de videovigilância como a falta de rede elétrica e internet o que torna quase inviável a existência de sistemas de videovigilância nesses locais. Dotar esses locais das infra estruturas necessárias poderia tornar-se demasiado dispendioso e os vigilantes humanos poderiam correr riscos no meio dos montes ou noutros locais remotos para além dos seus elevados custos.

Para além do problema dos roubos, existe um outro flagelo relacionado com os incêndios na floresta portuguesa, que todos os anos é dizimada pelo fogo devido a incêndios que surgem na sua maioria causados pelo homem sendo uma parte significativa os de origem criminosa.

Para dar resposta a estes problemas e no sentido de vigiar e dissuadir estes tipos de crimes, iniciamos um estudo que pretende propor um protótipo de um sistema de videovigilância para locais remotos (SVR - Sistema de Videovigilância Remota) de baixo custo de forma a diminuir o número de crimes e assim minimizar os prejuízos económico e sociais causados pelos mesmos.

Pretendemos estudar o problema e analisar tecnologias com potencial para propor uma solução que possa auxiliar a vigilância nesse tipo de locais com o pressuposto de poder vir a contribuir para a diminuição deste tipo de crimes devido ao seu efeito dissuasor pelo facto de se poder divulgar que estes locais já têm uma solução de vigilância oculta.

A solução proposta contempla um sistema de videovigilância com uma camara construída com base num *Raspberry Pi* onde o vídeo é transmitido em *streaming* via *Web* através de comunicações móveis. A alimentação do sistema nestes espaços sem energia elétrica é feita através de um painel fotovoltaico. É proporcionado ao utilizador uma interface para visualizar o vídeo transmitido e um mecanismo de notificações por *email*. É ainda possível a visualização de imagens gravadas num cartão de memória relativas a ocorrências de deteção de movimentos. Foram realizados inúmeros testes ao protótipo SVR sendo os resultados obtidos aqui descritos.

Keywords: video surveillance, SVR, Raspberry Pi, streaming, câmara, Web, internet.

Abstract

Since ancient times that men make surveillance of goods and commodities and more recently also from people in order to discouraging theft, vandalism and violence. In recent years, with the evolution of new technologies verified its adoption to assistance surveillance. Acts of terrorism that have taken place all over the world brought a climate of insecurity to the world population. This phenomenon, coupled with the high number of thefts and acts of violence led to the expansion of use of video surveillance means in order to discourage these kinds of crime may even, in some cases serve as evidence to punish the perpetrators thereof.

In Portugal has been verified escalating of crime in the most rural areas not only of goods such as agricultural implements but also fruit and even animals. These crimes predominate in rural places, relatively far from the villages and in places where there are not (or are practically non-existent) infrastructure necessary to implement video surveillance means such as lack of electricity grid and internet which makes almost impossible the existence of video surveillance systems in these places. Provide these local structures needed infrastructure could become too costly and human vigilantes could take risks among the hills or other remote locations in addition to its high costs.

Apart from the theft problem, there is another scourge related to forest fires in Portugal, which every year is decimated by fire because of fires that occur mostly manmade being a significant part of the criminal origin.

To respond to these problems and in order to monitor and deterring these kinds of crimes, we initiated a study that intends to propose a prototype of a video surveillance system for remote locations (SVR - Remote Video Surveillance System) low cost in order to reduce the number of crimes and so minimize the economic and social damage caused by them.

We intend to study the problem and analyze potential with technologies to propose a solution that can help surveillance in such places with the assumption of being able to contribute to reducing this type of crime because of its deterrent effect in that it is able to disseminate these places already have a covert surveillance solution.

The proposed solution includes a video surveillance system with a camera built on a Raspberry Pi where the video is broadcast in streaming via the *Web* through mobile communications. The system power in these spaces is done without electricity through a photovoltaic panel. It provided the user with an interface to view the transmitted video and a mechanism for email notifications. It is even possible to display images recorded to a memory card for the motion detection events. A large number of tests were performed to the SVR prototype and the results are described herein.

Keywords video surveillance, SVR, Raspberry Pi, streaming, camera, *Web*, internet.

Agradecimentos

Muitas foram as pessoas e instituições que contribuíram direta ou indiretamente para a efetivação deste trabalho, e, mesmo correndo o risco de esquecer alguém, não posso deixar de lhes expressar aqui os meus agradecimentos.

Em relação aos agradecimentos pessoais, não poderia deixar de começar pelo meu orientador, o Professor Doutor António Vieira de Castro, que, sempre me incentivou e demonstrou a sua confiança no meu trabalho e me apoiou na persecução dos objetivos que me propus atingir.

Ao meu grande amigo e colega Engenheiro Pedro Lima, que sempre me ajudou no que lhe foi possível e sempre teve uma palavra amiga de apoio e de incentivo para que este trabalho não ficasse a meio.

Ao colega e amigo Engenheiro Nuno Baptista, que sempre teve a disponibilidade para me ajudar e apoiar para que este trabalho fosse possível.

Um grande agradecimento aos meus colegas de trabalho do CeNTI – Centro de Nanotecnologia e Materiais Técnicos, Funcionais e Inteligentes, que sempre me deram a força necessária para prosseguir com este trabalho e finalizar esta etapa com o maior sucesso.

Ao ISEP (Instituto Superior de Engenharia do Porto) e ao DEI (Departamento de Engenharia Informática) que me proporcionou formação de qualidade e as condições de trabalho para eu investigar e desenvolver e assim tornar real este trabalho. E também por me dar todas as ferramentas para eu sobreviver no competitivo mundo do trabalho.

Por último, com um carinho muito especial, aos meus pais, pela confiança e encorajamento, há minha filha, a quem devo muito tempo, que ingratamente lhe roubei para terminar este trabalho.

A todos o meu muito obrigado.

Índice

1	Introdução	23
1.1	Enquadramento.....	23
1.2	O problema.....	24
1.3	Objetivos	28
1.4	Motivação	29
1.5	Estrutura da dissertação	30
2	A vigilância	33
2.1	Contextualização.....	33
2.1.1	A vigilância humana.....	34
2.1.2	Tecnologias de vigilância.....	34
2.2	A videovigilância	42
2.2.1	As câmaras de videovigilância.....	43
2.2.2	Locais de implementação da videovigilância.....	46
2.2.3	Enquadramento legal da videovigilância.....	52
3	O protótipo SVR - Sistema de Videovigilância Remota	55
3.1	Introdução.....	55
3.2	O modelo ADDIE	55
3.3	O modelo conceptual	57
3.4	Levantamento de requisitos e casos de uso	58
3.4.1	Levantamento de requisitos não funcionais	59
3.4.2	Levantamento de requisitos funcionais	61
3.4.3	Casos de uso	61
3.5	Análise de recursos e tecnologias.....	63
3.5.1	O linux Raspbian.....	63
3.5.2	O Apache2 Web Server	64
3.5.3	O Servidor Motion	64
3.5.4	O servidor de FTP Vsftpd.....	64
3.5.5	A linguagem de programação PHP	65
3.5.6	A linguagem HTML.....	66
3.5.7	O CSS.....	66
3.5.8	O Mysql	66
3.5.9	A linguagem de programação Python.....	67
3.5.10	O Bootstrap	67
3.5.11	O Raspberry Pi	68
3.5.12	Os Painéis fotovoltaicos	69
3.5.13	O controlador de carga	70
3.5.14	O conversor de tensão.....	70
3.6	Descrição técnica	70

3.6.1	Visão geral do sistema.....	71
3.6.2	Diagrama do sistema.....	71
3.6.3	Estudo do servidor de stream Motion	72
3.6.4	Desenvolvimento e apresentação do SVR	76
4	Testes e validação do sistema SVR	97
4.1	Testes realizados no desenvolvimento	97
4.2	Testes do protótipo SVR.....	100
4.2.1	Testes indoor ao sistema SVR	101
4.2.2	Testes outdoor do protótipo SVR.....	105
4.3	Avaliação do sistema de videovigilância SVR.....	108
4.3.1	Camuflagem do protótipo SVR	108
4.3.2	Facilidade de montagem	109
4.3.3	Autonomia de bateria	110
4.3.4	Recuperação do sistema numa falha total de energia elétrica	111
4.3.5	Envio de notificação na deteção de movimento.....	112
4.3.6	Espaço ocupado em disco pelos vídeos/imagens capturadas	113
4.4	Análise geral ao protótipo SVR	114
5	Conclusões e trabalho futuro	123
5.1	Conclusões e análise crítica	123
5.2	Trabalho Futuro	125
5.3	Considerações finais	126
6	Anexos.....	131
6.1	Anexo 1 -Mockup da primeira versão da página <i>Web</i>	131
6.2	Anexo 2 - Mockup da segunda versão da página <i>Web</i>	133
6.3	Anexo 3 - Questionário de avaliação do protótipo	135
6.4	Anexo 4 - Opções do servidor de stream.....	139
6.5	Anexo 5 - Especificadores de texto aceites pelo servidor.....	151

Lista de Figuras

Figura 1 - Exemplo de notícia sobre o roubo de azeitona no Alentejo	25
Figura 2 - Exemplo de notícia sobre o roubo de gado	26
Figura 3 - Exemplo de notícia sobre fogo em Portugal	26
Figura 4 - Exemplo de notícia sobre fogo em Portugal	27
Figura 5 - Exemplo de um local isolado.....	28
Figura 6 - A vigilância humana	34
Figura 7 - Primeiro sistema de CCTV	35
Figura 8 - Sistema de CCTV, com gravação de video	35
Figura 9 - Sistema de CCTV com gravação e multiplexer	36
Figura 10 - Sistema CCTV com gravação de video em formato digital	37
Figura 11 - CCTV com ligação por cabo <i>ethernet</i>	37
Figura 12 - Sistema de CCTV com comunicação sem fios	38
Figura 13 - Sistema de reconhecimento de matrículas.....	38
Figura 14 - Imagem térmica em escuridão total.....	39
Figura 15 –Um drone e um VANT da polícia Portuguesa	40
Figura 16 - NeoFace Watch	41
Figura 17 - Câmara LTL5210A.....	44
Figura 18 - Spypoint Mini Live and Live 4G Wildlife Câmara.	44
Figura 19 – A Spypoint Mini Live and Live 4G Wildlife Câmara.	45
Figura 20 - Notícia sobre videovigilância urbana na Amadora.	46
Figura 21 - Videovigilância na ribeira Porto	47
Figura 22 - Videovigilância em loja comercial	48
Figura 23 – Sistema de videovigilância para aeroportos	50
Figura 24 - Sistema de videovigilância em autoestradas	51
Figura 25 - Sistema de videovigilância de um estádio desportivo.....	52
Figura 26 - Modelo ADDIE	56
Figura 27 - O modelo conceptual do SVR.....	58
Figura 28 - Diagrama de caso de uso da camera de video-vigilância	62
Figura 29 - Diagrama de sequencia de autenticação e download arquivo	63
Figura 30 - Raspberry Pi versão 2.0.....	69
Figura 31 - Dimensões do Raspberry Pi 2.0.....	69
Figura 32 - Diagrama do Sistema de Videovigilância	71
Figura 33 - Página de configuração do servidor <i>Motion</i>	76
Figura 34 - Janela de autenticação de utilizador.....	81
Figura 35 - Página principal com acesso ao vídeo stream	81
Figura 36 - Janela de alteração de credenciais de acesso.....	82
Figura 37 - Janela de listagem de vídeos e imagens	83
Figura 38 - Janela de inserção de correio eletrónico para notificações.....	84
Figura 39 - Versão 2 da janela de autenticação de utilizador	84
Figura 40 - Versão 2 da página principal com acesso ao vídeo <i>streaming</i>	85

Figura 41 - Versão 2 da página de alterar as credenciais de acesso	85
Figura 42 - Versão 2 da página de listar o arquivo de imagens e vídeos	86
Figura 43 - Versão 2 da página de altera correio eletrónico das notificações	86
Figura 44 - Página de configurações do servidor	87
Figura 45 - Tabela de utilizadores	87
Figura 46 - Tabela de armazenamento de os dados para o envio de notificações	88
Figura 47 - Seleção do servidor de <i>Web</i>	88
Figura 48 - Utilização do <i>dbconfig-common</i>	89
Figura 49 - Conversor DC-DC STEP-UP	90
Figura 50 - Controlador de carga.....	91
Figura 51 - Bateria LiPo.....	92
Figura 52 - Raspberry Pi com a Picam	92
Figura 53 - Todos os componentes da câmara <i>assembled</i>	93
Figura 54 - Painéis fotovoltaicos	93
Figura 55 - Esquema de ligação painéis fotovoltaicos.....	94
Figura 56 - Estrutura camuflada do sistema de videovigilância SVR.....	95
Figura 57 - O SVR a vigiar um local de acesso	96
Figura 58 - Página com <i>streaming</i> de vídeo	97
Figura 59 - <i>Email</i> de notificação	98
Figura 60 - Página de configuração do <i>Servidor Motion</i>	98
Figura 61 - <i>Streaming</i> de vídeo na versão 2 da página <i>Web</i>	99
Figura 62 - Câmara de videovigilância e painel fotovoltaico.....	99
Figura 63 - Local a ser vigiado pela câmara de videovigilância	100
Figura 64 - Imagem do vídeo capturado pela câmara de vigilância.....	100
Figura 65 - Sensibilidade à intrusão em espaços interiores	101
Figura 66 - Ocorrências de intrusão durante testes num espaço interior	102
Figura 67 - Vídeo gerado pelo SVR com todas as ocorrências de intrusão	102
Figura 68 - Vídeo gerado pelo SVR	103
Figura 69 - Dados adicionados ao vídeo (data e hora).....	103
Figura 70 - Mecanismo de navegação no <i>player</i> do vídeo	103
Figura 71 – Lista de vídeos na máquina do utilizador após <i>download</i>	104
Figura 72 - Testes indoor do sistema SVR em uma sala de aula	104
Figura 73 – Teste à área de intrusão	105
Figura 74 - Cruzamento com sistema SVR instalado.....	106
Figura 75 – Imagem capturada pelo SVR em teste	106
Figura 76 - Local de acesso com o sistema SVR instalado.....	107
Figura 77 – Imagem capturada pelo SVR em teste em um local de acesso	107
Figura 78 - Estrutura camuflada do sistema de videovigilância SVR.....	109
Figura 79 Mockup da página <i>Web</i>	131
Figura 80 Mockup 2 versão página <i>Web</i>	133

Lista de código

Código 1 – Configuração servidor vsftpd	77
Código 2 – Configuração servidor Apache2	78
Código 3 – Configuração do Servidor Motion	78
Código 4 - Configuração do cliente dns ddclient	79
Código 5 - Script Python de envio de notificações.....	80

Lista de Tabelas

Tabela 1 - Descrição de casos de uso	62
Tabela 2 - Tabela de parametrizações do servidor	74
Tabela 3 - Tabela de eventos do servidor	74
Tabela 4 Tabela de análise das detecções de movimento.	112
Tabela 5 Tabela de todas as opções do Servidor Motion	149
Tabela 6 Tabela de todos especificadores de texto aceites pelo Servidor Motion	153

Lista de Gráficos

Gráfico 1 - Distribuição da população alvo quanto ao sexo	114
Gráfico 2 - Distribuição da população alvo quanto à idade	115
Gráfico 3 - Distribuição da população alvo quanto às habilitações literárias.....	115
Gráfico 4 - Percentagem de inquiridos que já tiveram contacto com sistemas de videovigilância	116
Gráfico 5 - Percentagem de inquiridos que acham os sistemas de videovigilância para locais remotos uteis	116
Gráfico 6 - Percentagem de inquiridos possivelmente adquiriria um sistema de videovigilância para locais remotos.....	117
Gráfico 7 - Percentagem de inquiridos que acha importante a camuflagem no sistema de videovigilância	117
Gráfico 8 – Distribuição da população alvo em relação à camuflagem do protótipo SVR.	118
Gráfico 9 – Distribuição da população alvo em relação à montagem do protótipo SVR.....	118
Gráfico 10 – Distribuição da população em relação à usabilidade do protótipo SVR	119
Gráfico 11 – Distribuição da população em relação à inovação do protótipo SVR	119
Gráfico 12 - Distribuição da população em relação à qualidade de imagem do protótipo SVR	120
Gráfico 13 – Distribuição da população em relação à deteção de movimento pelo protótipo SVR	121

Notação e glossário

Lista de Acrónimos

2G	<i>Second generation of mobile telecommunications technology</i>
3G	<i>Third generation of mobile telecommunications technology</i>
4G	<i>Fourth generation of mobile telecommunications technology</i>
AONT	<i>Aeronaves de Observação Não Tripuladas</i>
CAT5	<i>Cabo entrelaçado</i>
CENTI	<i>Centro Nanotecnologia Materiais Técnicos, Funcionais e Inteligentes</i>
CNPD	<i>Comissão Nacional de Protecção de Dados</i>
CPU	<i>Central Processing Unit</i>
CSI-2	<i>Camera Serial Interface</i>
CSS	<i>Cascading Style Sheets</i>
CRON	<i>Command Run On Notice</i>
DEI	<i>Departamento de Engenharia Informática</i>
DL	<i>Decreto de lei</i>
DNS	<i>Domain Name System</i>
DR	<i>Diário da Republica</i>
FTP	<i>File Transfer Protocol</i>
GPS	<i>Global Positioning System</i>
HTML	<i>Hypertext Markup Language</i>
HTTP	<i>Hypertext Transfer Protocol</i>
IP	<i>Internet Protocol</i>
ISEP	<i>Instituto Superior de Engenharia do Porto</i>
JPG	<i>Joint Photographics Experts Group</i>

JS	<i>JavaScript Syntax</i>
LiPo	<i>Lithium polymer battery</i>
MIPI	<i>Mobile Industry Processor Interface</i>
MMPT	<i>Maximum power point tracking</i>
MMS	<i>Multimedia Messaging Service</i>
MySQL	<i>Structured Query Language</i>
PPM	<i>Portable Pixel Map</i>
PPPD	<i>Point to point protocol daemon</i>
SGBD	<i>Sistemas de Gestão de bases de dados</i>
SIG	<i>Geographic Information System</i>
TCP	<i>Transmission Control Protocol</i>
SVR	<i>Sistema videovigilância Remoto</i>
www	<i>World Wide Web</i>
Vac	<i>Tensão alternada</i>
Vdc	<i>Tensão contínua</i>
VANT	<i>Veículo Aéreo Não Tripulado</i>

1 Introdução

*“Como é necessária a vigilância na guerra,
é também preciso maior cuidado na paz.”*

António Vieira

No presente capítulo apresenta-se o enquadramento geral relacionado com o tema em análise neste trabalho, evidenciando a necessidade de vigilância de pessoas e bens na sociedade moderna.

Expõe-se a dificuldade da vigilância em locais remotos concretamente em zonas sem eletricidade ou acesso á internet, como sendo o principal problema a estudar e definem-se o objetivo do presente estudo que visa focalizar o desenvolvimento de um protótipo com potencial para solucionar o problema identificado.

Apresenta-se a motivação do autor e termina-se o capítulo com a organização do presente documento.

1.1 Enquadramento

A vigilância de pessoas e mercadorias sempre esteve intrinsecamente presente na sociedade e foi evoluindo e adaptando-se à evolução tecnológica. No começo a vigilância era feita apenas por vigilantes humanos que faziam a vigília de pessoas e bens, mas esta era uma opção que acarretava custos elevados e punha por vezes em causa a vida humana devido aos elevados riscos a que estes profissionais estavam sujeitos.

Apareceram entretanto novas tecnologias como as câmaras de vigilância, o GPS, a internet e as comunicações móveis (GSM,GPRS,UMTS), que foram rapidamente introduzidas na vigilância de pessoas e bens, dado que a sua utilização se traduz numa redução de meios humanos para além de ser uma vigilância mais eficiente e com o complemento de funcionar como elemento dissuasor de crimes.

Nos últimos anos houve uma massificação dos sistemas de videovigilância que passaram a ser utilizados nos mais diversos locais, devido ao clima de insegurança e medo que as pessoas sentem em consequência do crescimento de alguns crimes como assaltos, vandalismo e situações de violência.

Existem muitos locais que carecem de sistemas de videovigilância devido à ausência de infraestruturas como energia elétrica e rede internet onde a vigilância humana seria uma opção altamente dispendiosa. Esses locais têm vindo a ser alvo de crimes diversificados em que os seus autores saem impunes. Estes crimes traduzem-se em prejuízos avultados, vidas humanas em risco e um elevado clima de insegurança e de medo.

Sendo a videovigilância uma forma de dissuadir e diminuir o número de crimes, com o presente estudo pretendemos desenvolver um sistema de videovigilância para locais onde não existe qualquer tipo de vigilância seja ela humana ou tecnológica devido a fatores como a ausência das infraestruturas necessárias. Existem locais, normalmente situados em zonas rurais onde não existe rede de energia elétrica, nem rede cablada ou *wifi* de acesso à internet sendo economicamente inviável a existência de um vigilante. Pretende-se estudar a possibilidade de dar uma resposta a este problema através do desenvolvimento de um sistema de videovigilância autónomo de energia elétrica com recurso às energias renováveis e para contornar o problema do acesso à internet será utilizado uma rede de comunicações móveis(2G,3G,4G) sempre que possível, caso contrário a informação será gravada em cartão de memória.

Com o decorrer deste estudo pretendemos desenvolver um protótipo com uma câmara de videovigilância, que permita a transmissão de vídeo em *streaming* através de um *modem* de dados para comunicação através das redes móveis e seja autónomo no que respeita à energia elétrica á energia solar através de um painel fotovoltaico. Pretendemos, apos o desenvolvimento verificar o potencial do protótipo, estudando a possibilidade de num futuro próximo o transformar num produto comercial, para um segmento bastante específico como a vigilância de locais isolados, remotos, essencialmente rurais e com ausência de qualquer tipo de vigilância devido a problemas técnicos e económicos

1.2 O problema

Nos últimos tempos temos constatado que inúmeros locais mais isolados foram alvo de furtos. Foram furtadas colheitas de azeitonas, alfaias agrícolas, gado, leite, entre outros. O problema dos locais onde decorreram estes incidentes é o facto de se encontrarem deslocados das povoações, sendo de notar a inexistência de pessoas para estar constantemente a vigiar estes locais ou para estar atentas a movimentações estranhas.

Alguns destes locais também não dispõem de energia elétrica nem de uma rede de dados o que torna os sistemas de videovigilância convencionais impróprios para estes locais. Nas Figuras 1, 2 e 3 apresentamos algumas notícias que mostram a realidade do problema mencionado.



Figura 1 - Exemplo de notícia sobre o roubo de azeitona no Alentejo ¹

Nesta notícia primeira notícia Figura 1 é possível perceber que os agricultores alentejanos têm sido vítimas de assaltos nas suas explorações. Os grupos de assaltantes colheram a azeitona durante a noite provocando aos proprietários e agricultores enormes prejuízos.

Partimos para o presente estudo com o pressuposto de que com o sistema de videovigilância, que propomos seria possível ajudar a identificar os autores dos furtos, assim como também seria possível enviar um alerta aos agricultores e proprietários a partir do momento em que foi detectado movimento naquele local de monitorização. Deste modo consideramos poder ser possível apanhar os criminosos em flagrante no momento do delito através da notificação às autoridades competentes (polícia), ou em alternativa ficar em posse de elementos e informações visuais (fotos e vídeos) sobre a ocorrência para entregar às autoridades.

Um outro flagelo, no que concerne à criminalidade em espaços rurais é o roubo do gado que, como se pode ver na Figura 2 tem assumido em Portugal uma dimensão considerável já cerca de dois mil bovinos roubados.

¹ Disponível em <http://sicnoticias.sapo.pt/pais/2013-12-16-agricultores-de-campo-maior-queixam-se-de-roubos-de-azeitonas;jsessionid=CB6D13CD06053C0839F0D06B75E89747>

REDES ORGANIZADAS

Roubo de gado passa o milhão de euros

por ROBERTO DORES 19 julho 2010 4 comentários



Mais de dois mil bois e vacas roubados em dois anos estão a levar produtores ao desespero.

O roubo de gado em Portugal disparou nos últimos dois anos, lançando o desespero entre os produtores pecuários. Segundo uma estimativa da Associação Nacional de Engordadores Bovinos (ANEBO), terão sido roubados perto de dois mil bois e vacas, prejuízo que supera um milhão de euros. Apesar de recentemente um grupo de produtores se ter juntado para desvendar uma das redes, radicada no norte do País e que actua entre o Ribatejo e o Alentejo, ainda não há qualquer detenção, embora as autoridades já tenham identificado vários indivíduos.

Figura 2 - Exemplo de notícia sobre o roubo de gado ²

À semelhança de outros países Europeus, Portugal é extremamente afetado pela calamidade dos incêndios. Todos os anos existem milhares de fogos, sendo na sua grande maioria de origem humana, quer por negligência ou acidente (queimadas, queima de lixos, lançamento de foguetes, cigarros mal apagados, linhas eléctricas), quer intencionalmente (com origem criminosa).

Nos casos de incendios com origem criminosa é raro serem apanhados os culpados.

Fogos com falhas mas sem culpados



por Sónia Graça

29 de Dezembro, 2013



Figura 3 - Exemplo de notícia sobre fogo em Portugal ³

² Disponível em http://www.dn.pt/inicio/portugal/interior.aspx?content_id=1621307

³ Disponível em <http://www.sol.pt/noticia/95820>

Os incêndios com origem em causas naturais(trovoadas), correspondem a uma pequena percentagem do numero total de ocorrências conforme podem ver no gráfico da figura 4, sendo as principais fatias para a negligencia(39%), para a origem criminosa(23%) ou por factores desconhecidos(37%).



Figura 4 - Exemplo de notícia sobre fogo em Portugal ⁴

Os incêndios são um grande problema económico, ambiental e social em Portugal e no mundo pelo que devem ser tomadas medidas de prevenção e de dissuasão deste tipo de crimes.

Uma das medidas que poderia ajudar a reduzir o número de incêndios e a área degradada por eles seria a implementação de sistemas de videovigilância. O sistema de videovigilância que propomos e que será desenvolvido no âmbito desta dissertação de mestrado poderá ser, um meio alternativo de combate a este tipo de crimes e acidentes pois será possível ver a imagem em tempo real dos locais em questão, assim como receber notificações de quando existir algum tipo de movimento (intrusão) nestes locais, sendo eventualmente possível detetar o início de alguns incêndios e se este tiver início em mãos criminosas possivelmente vir a identificar o suspeito ou até proporcionar que seja apanhado em flagrante delito. O facto de ser detetado o foco de incêndio mais cedo, poderá permitir que este seja combatido mais facilmente e eficazmente o que pode resultar numa área queimada muito mais reduzida, implicando uma diminuição dos prejuízos económicos, ambientais e sociais.

⁴ Disponível em:
<http://www.prociv.pt/RISCOSVULNERABILIDADES/RISCOSNATURAIS/INCENDIOSFLORESTAIS/Pages/Causas.aspx>

Pretendemos que o sistema de videovigilância que propusemos seja o mais furtivo e invisível possível pelo que para tal, o seu *design* terá de ser pensado de forma camuflada para que seja possível misturar-se com o ambiente em que seja colocado.

Como o sistema de videovigilância foi pensado para ser colocado em locais remotos, e atendendo ao facto destes locais terem normalmente elementos característicos como árvores, pedras, vegetação, idealizamos uma caixa/estrutura para envolver todos os restantes componentes com a forma de uma rocha (pedra).

Na Figura 5, pode-se ver um exemplo de um local onde poderia ser colocado o nosso protótipo com uma camara de videovigilância. É um local remoto que é apenas atravessado por um caminho e que pode ser utilizado para acesso a locais onde existem bens e produtos prontos a ser alvo de crime. A câmara de videovigilância poderia ser colocada estrategicamente de forma a ser possível a identificar quem passa nesse local no sentido de entrada da povoação aos campos ou de forma a capturar rostos em ambos os sentidos.



Figura 5 - Exemplo de um local isolado

As vias de acesso em locais isolados são utilizados para cometer delitos que podem ser combatidos através de uma melhor vigilância utilizando para isso o sistema que nos propusemos a desenvolver.

1.3 Objetivos

O objetivo do presente estudo desenvolvido no âmbito desta tese de mestrado, consta em analisar, estudar e desenvolver um sistema de videovigilância para locais remotos, sem energia elétrica que possa transmitir vídeo em tempo real através de um *modem* de

dados para que seja possível assistir vídeo em qualquer parte do mundo, desde que exista uma ligação à *internet ao que se está lá a passar*. Este sistema de videovigilância deverá ser portátil, de fácil instalação, robusto, sem necessidade de ligação à rede elétrica e de baixo custo.

No sentido de alcançar os objetivos propostos considerámos ser necessário estudar diversas tecnologias de informação nomeadamente: servidores de vídeo, formatos de transmissão de vídeo, linguagens de programação *Web* (cliente/servidor), linguagens de *script* e bases de dados. Para além destas será necessário investigar e integrar diversas tecnologias de forma a ter um *hardware* capaz de capturar e processar vídeo e que possa ser alimentado através de uma fonte de energia renovável (painel solar) e dispor de uma ligação à internet através de um *modem* de dados.

Para a construção deste sistema será feita a instalação de um servidor de *streaming* que permite a aplicação de algoritmos de deteção de movimento, bem como utilizar diversos *scripts* para adotar diversas funcionalidades, tais como armazenar vídeos em diferentes formatos e em locais específicos e ainda enviar *emails* de aviso e notificação. Será feito o desenvolvimento de uma página *Web* que permite ver o vídeo que está a ser transmitido em *streaming* bem como efetuar diversas configurações para a sua visualização.

1.4 Motivação

Como autor do presente estudo tornei-me um aficionado por tecnologia desde pequenino, principalmente devido a um episódio que ainda recorda com carinho; “um dia chega o meu pai ao pé de mim e deu-me uma revista de eletrónica mal sabia eu ler e escrever, mas houve qualquer coisa que me chamou a atenção e desde esse dia todos os meus passos foram dados de forma a seguir o caminho na área das novas tecnologias”. No secundário em vez de seguir a área científico natural ingressei pela área tecnológica, onde tirei o curso de eletrotécnica e eletrónica de nível 3 da Escola Secundária de Carregal do Sal, no ensino superior ingressei no curso de engenharia eletrotecnia - eletrónica e de computadores do Instituto Superior de Engenharia do Porto onde obtive a minha licenciatura. Pretendendo aprender mais principalmente na área de informática optei por me inscrever no mestrado em engenharia informática no ramo de sistemas gráficos e multimédia.

Para a conclusão do curso de mestrado é necessário o desenvolvimento de uma dissertação em que se pretende dar a resposta a um problema que exista e logo me lembrei de um que têm sido constantemente focado pelos média que é o problema dos casos de furto nas zonas rurais de gado, fruta e outras colheitas bem como assaltos em locais distantes, remotos, sem qualquer tipo de vigilância devido a problemas económicos e ausência de infra estruturas para adotar as mais recentes tecnologias de vigilância.

Como a minha formação é na área da eletrónica e da informática deliberei que havia algo que eu poderia fazer para minimizar este problema e trazer um pouco de mais segurança e bem-estar à sociedade. Então propusemos como tese de mestrado um sistema de videovigilância para locais remotos. Tenho como principal motivação não só terminar o mestrado em informática - Sistemas Gráficos e Multimédia, mas principalmente dar uma solução a este problema que tantos transtornos e prejuízos traz á nossa sociedade. Espero que com este sistema consiga encontrar uma solução que minimize o número de crimes que são realizados em locais sem vigilância e assim tornar o nosso mundo em um local mais seguro para todos nós como cidadãos e assim ser possível viver com mais qualidade sem ter presentes os mais diversos sentimentos de insegurança.

Para além dos assaltos existe também o flagelo dos incêndios que todos os anos causam vítimas humanas e destroem milhares de hectares de floresta o que se traduz em prejuízos económicos elevados, danos humanos e ambientais irreparáveis. Esta dissertação de mestrado pode não ser a solução mas se eu puder contribuir para minimizar este flagelo mesmo que numa mínima parte para mim será motivador e dá-me vontade de levar este trabalho académico até ao fim e quem sabe torná-lo num produto de mercado com capacidade de dissuadir este tipo de crimes e também ajudar na redução da área ardida através da deteção de incêndios ainda no seu início.

1.5 Estrutura da dissertação

A presente dissertação é constituída por 5 capítulos e 5 anexos, cujo conteúdo se descreve em seguida:

No primeiro capítulo é feito o enquadramento da dissertação e o levantamento de um problema a que se pretende dar uma possível solução. Também é efetuada a descrição dos principais objetivos propostos e qual a motivação da realização deste trabalho.

No segundo capítulo é feita a contextualização da vigilância, em que apresentamos a vigilância humana e a vigilância com auxílio de tecnologias. Apresentamos também a videovigilância como sendo o futuro da vigilância e os locais onde esta é utilizada bem como o seu enquadramento legal.

No terceiro capítulo é apresentado o modelo conceptual do protótipo de videovigilância (SVR), que é proposta de solução ao problema apresentado. É efetuado o levantamento de todos os requisitos funcionais e não funcionais que o protótipo deverá cumprir e serão analisadas as diferentes tecnologias que serão utilizadas. Neste mesmo capítulo será feita a descrição, implementação e desenvolvimento do protótipo de videovigilância (SVR).

No Quarto capítulo são demonstrados os diferentes testes efetuados durante e no final do desenvolvimento do protótipo SVR, como todas as validações e avaliações do mesmo. Por último no quinto capítulo são apresentadas todas as conclusões referentes a todo o trabalho desenvolvido, bem como uma análise critica, uma breve descrição de trabalhos futuros a realizar para melhoramento deste protótipo apresentado como solução ao problema identificado neste estudo e também algumas considerações finais sobre o trabalho desenvolvido.

Relativamente aos anexos, estes encontram-se divididos da seguinte forma:

- Anexo 1 - *Mockup* da primeira versão da página *Web*;
- Anexo 2 - *Mockup* da segunda versão da página *Web*;
- Anexo 3 - Questionário de avaliação do protótipo;
- Anexo 4 – Tabela com apresentação de todas as funcionalidades do servidor *Motion*;
- Anexo 5 – Especificadores de texto reconhecidos pelo servidor *Motion*.

2 A vigilância

“O preço da liberdade é a vigilância eterna.”

Thomas Jefferson

No presente capítulo apresenta-se a contextualização da vigilância referindo-se a vigilância humana com um vigilante e a vigilância mediada por as tecnologias de apoio à vigilância. Apresenta-se a videovigilância como sendo a vigilância do futuro em que se descreve o seu modelo e evolução desde o seu aparecimento até à atualidade, são apresentados exemplos de locais em que esta é empregue e o seu enquadramento legal.

2.1 Contextualização

A questão segurança como defesa, sensação de estar seguro, protegido contra os riscos é tão antiga quanto a existência do homem. Com a evolução do mundo, os riscos foram aumentando e já no século XVI, na Inglaterra, surgiram os primeiros “vigilantes”. Eram pessoas escolhidas por serem hábeis na luta e no uso da espada, remunerados por senhores feudais, com recursos provenientes dos impostos cobrados aos cidadãos. Já no antigo velho oeste americano existiam pessoas que escoltavam as caravanas que poderíamos classificar como seguranças privadas.

Em 1820 nos Estados Unidos, Allan Pinkerton organizou um grupo de homens para dar proteção ao então presidente Abraham Lincoln desse modo foi criada a primeira empresa de segurança privada do mundo. Foi apenas no século XIX, em 1852, que devido às deficiências naturais do poder público, os americanos Henry Wells e William Fargo criaram oficialmente a primeira empresa de segurança privada do mundo.

A vigilância pode ser dividida em duas grandes categorias. A vigilância através de meios humanos em que a figura central é o vigilante em que este têm o dever de vigiar e zelar pela segurança das estruturas, bens e pessoas e a vigilância através de meios tecnológicos, em que são utilizadas tecnologias como a videovigilância, GPS, *video streaming*, *face tracking*, reconhecimento matrículas, videovigilância remota, câmaras térmicas, vigilância com Aeronaves de Observação não Tripuladas (AONT) e drones.

2.1.1 A vigilância humana

Desde os primórdios que a figura de vigilante surgiu, como forma de persuadir e minimizar os atos de vandalismo, roubos, atos de terrorismo, violência, ofensas físicas e corporais.



Figura 6 - A vigilância humana ⁵

No entanto, em espaços grandes, como escolas, fábricas ou armazéns, o vigilante não poderia estar em todos os locais, sendo obrigado muitas das vezes a abandonar o seu posto de trabalho para fazer uma ronda ao espaço envolvente criando nessas ocasiões falhas de segurança de vigilância.

Não podia estar ao mesmo tempo em vários locais até que, com o desenvolvimento da tecnologia surgiram os primeiros sistemas de apoio aos vigilantes conhecidos por sistemas CCTV (*Closed-circuit-television*).

2.1.2 Tecnologias de vigilância

Neste ponto pretendemos descrever algumas das tecnologias utilizadas pelos sistemas de videovigilâncias mais evoluídos e mais complexos que permitem auxiliar a vigilância de forma a esta ser mais eficiente e eficaz e assim ajudar a trazer o sentimento de segurança a sociedade.

Nos pontos em seguida apresenta-se a evolução dos sistemas de videovigilância desde o seu aparecimento até aos dias atuais bem como uma descrição dos locais onde são

⁵ Disponível em: <http://contraparte.mx/wp-content/uploads/2014/07/caseta1.jpg>

instalados diferenciados por categorias e no final é feito o enquadramento legal da videovigilância.

2.1.2.1 O CCTV

Em 1950 apareceu o primeiro sistema de vídeo vigilância que era um sistema bastante simples, constituído apenas por uma televisão e uma câmara conectadas por um cabo coaxial.

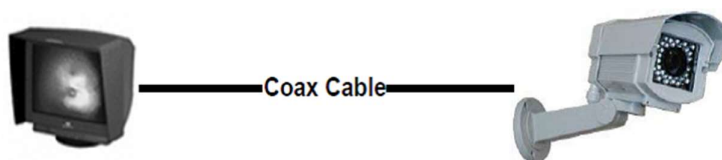


Figura 7 - Primeiro sistema de CCTV ⁶

Estes sistemas eram compostos por uma ou mais câmaras de vídeo e uma televisão. O vigilante poderia estar num local onde deveria olhar para o televisor este mostrava as imagens das câmaras de vídeo colocadas em locais estratégicos permitindo assim que uma única pessoa conseguisse vigiar uma maior zona e em maior segurança.

Perante alguma ocorrência, o vigilante poderia atuar ou acionar os meios necessários para garantir a segurança das pessoas e bens.

Com o aparecimento do gravador de cassetes em 1970, foi possível passar a gravar o sinal de vídeo para futura visualização. Esta solução ainda era bastante primitiva e consistia numa câmara ligada ao gravador de cassetes e este ligado a um televisor.

Normalmente cada câmara estava ligada a um videogravador que por sua vez estava ligado a uma televisão (Figura 8).



Figura 8 - Sistema de CCTV, com gravação de vídeo

⁶ Disponível em:

<http://www.readynas.com/download/archive/pdf/Video%20Surveillance%20White%20Paper.pdf>

Esta configuração permitia, diminuir o erro humano, porque todas as imagens eram gravadas, sendo possível revê-las posteriormente.

Este sistema tinha vários inconvenientes, tais como, as fitas das cassetes, que eram frágeis e acabavam por partir. Cada cassete só permitia duas horas de gravação, logo era necessário trocar a cassete várias vezes durante o dia.

Para monitorizar um local em que eram necessárias várias câmaras, o sistema não era economicamente viável, como tal apareceu uma solução para este problema, o *multiplexer* que permitia ter várias câmaras ligadas a um único vídeo e monitor, fazendo a comutação entre as câmaras. Assim foi possível aumentar o sistema sem comprometer os seus requisitos.

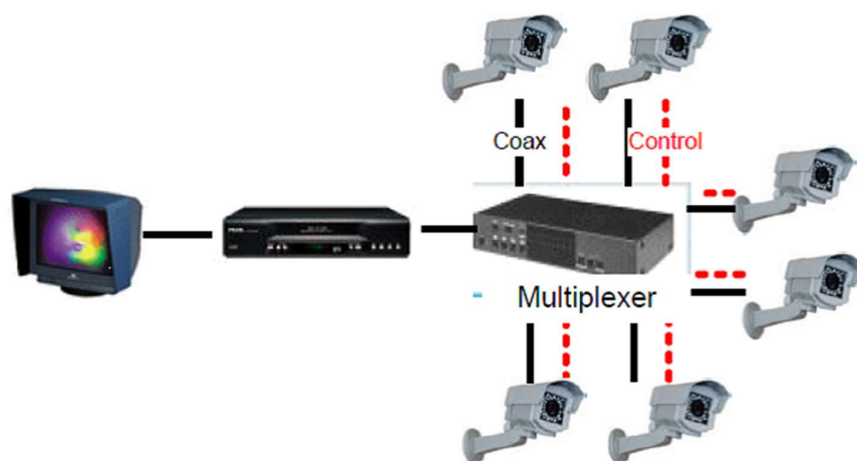


Figura 9 - Sistema de CCTV com gravação e multiplexer ⁷

Com a evolução da tecnologia foi possível apresentar, o sinal de várias câmaras no mesmo monitor e alternar com diferentes grupos de câmaras. O que permitiu uma maior monitorização devido ao maior número de câmaras envolvidas.

Com os *DVR*'s passou a ser possível converter o sinal de vídeo analógico em digital e gravar o vídeo em formato digital. Como o sinal digital é mais confiável, fiável para transmitir e gravar, rapidamente se tornou a tecnologia preferida, para além disso tornou possível estar a visualizar o vídeo guardado, mesmo quando este continua a gravar sendo que grava uma quantidade maior de vídeo.

⁷Disponível em:

<http://www.readynas.com/download/archive/pdf/Video%20Surveillance%20White%20Paper.pdf>

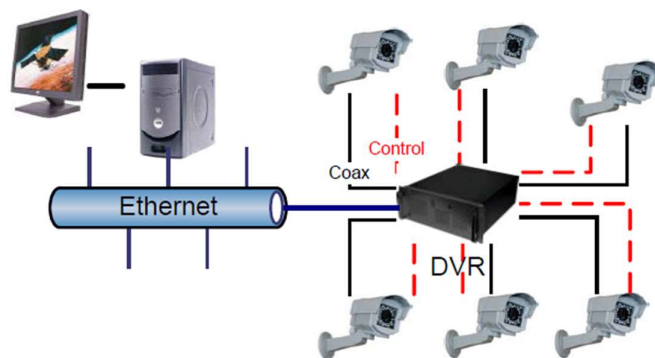


Figura 10 - Sistema CCTV com gravação de vídeo em formato digital⁸

Com o aparecimento da conversão do sinal de vídeo em digital novas tecnologias puderam começar a ser integradas, tais como protocolos de internet e compressão de vídeo (*codecs*).

Grande parte das empresas já dispunham de uma infraestrutura de comunicação em rede *Ethernet* utilizando cabo CAT5, que se tornou-se o meio *Standard* para ligação das câmaras e o protocolo TCP/IP utilizado na comunicação dos pacotes de dados.

É possível comprimir os dados digitais do vídeo de forma a reduzir o seu tamanho, logo começaram a aparecer algoritmos de compressão em que o MPEG rapidamente se tornou o preferido e adotado por grande parte deste tipo de sistemas.

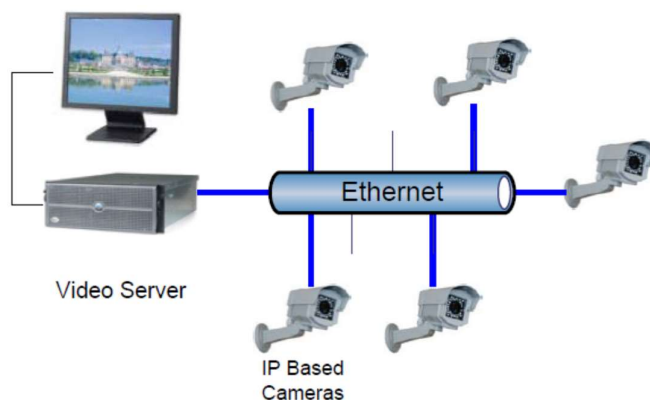


Figura 11 - CCTV com ligação por cabo *ethernet*

O aparecimento da tecnologia sem fios fez com que os sistemas de videovigilância também evoluíssem e passassem a emigrar para esta tecnologia o que tornou mais fácil a instalação destes sistemas em edifícios que já se encontram construídos não sendo necessário qualquer intervenção elétrica.

⁸ Disponível em:

<http://www.readynas.com/download/archive/pdf/Video%20Surveillance%20White%20Paper.pdf>

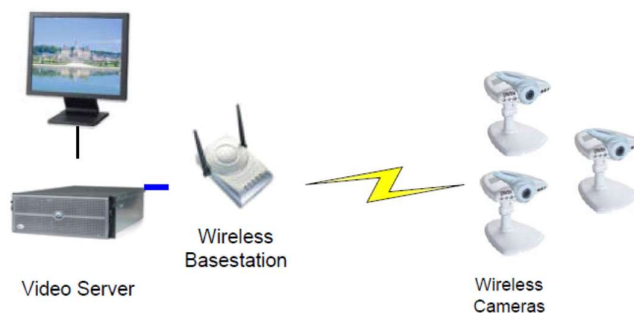


Figura 12 - Sistema de CCTV com comunicação sem fios⁹

2.1.2.2 O reconhecimento de matrículas

Os sistemas de reconhecimento automático de matrículas (ANPR) capturam imagens de veículos e reconhecem a seu número de matrícula. Estes sistemas são utilizados na ajuda na deteção de carros roubados principalmente quando instalados em autoestradas e utilizam algoritmos como, *Edge Finding Method* e *Window Filtering Method*[Kranthi, Pranath, Srisail,2011].

Esta tecnologia também é utilizada em locais em que é necessário fazer o controlo de acessos de veículos em que o sistema após o reconhecimento da numero de matricula verifica na base de dados se este têm permissão de acesso ao local.

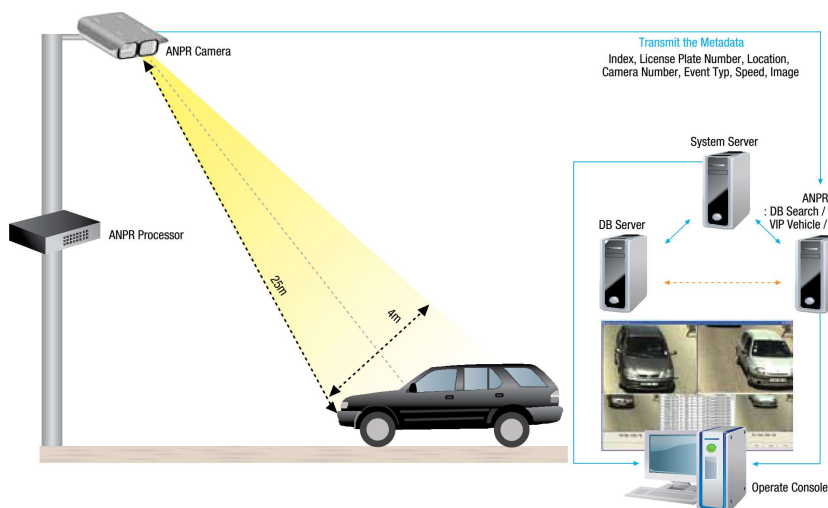


Figura 13 - Sistema de reconhecimento de matrículas¹⁰

⁹Disponível em:

<http://www.readynas.com/download/archive/pdf/Video%20Surveillance%20White%20Paper.pdf>

¹⁰Disponível em: http://www.samsungsecurity.com/_img/menu4/12_SISS_catalog_120328_E_F.pdf

2.1.2.3 A vigilância remota

A videovigilância remota consiste na capacidade deste tipo de sistemas enviar o vídeo capturado pelas câmaras para *internet* de forma a ser possível visualiza-lo em qualquer parte do mundo, mas também a possibilidade de controlar este tipo de sistemas à distância. As câmaras destes sistemas tem um interface de rede cablada ou *modem* de dados para que sejam possível liga-las á *internet*.

2.1.2.4 As câmaras Térmicas

Imagem térmica é uma das tecnologias que se desenvolveu e passou a ser parte integrante dos sistemas de videovigilância pois torna possível ver nas mais adversas condições nomeadamente em ambientes noturnos.

Esta tecnologia consiste em medir as variações de temperatura e da radiação térmica emitida por um objeto e por aquilo que está a sua volta. Estas câmaras térmicas podem ser utilizadas em qualquer ambiente e tanto durante o dia como durante a noite.

No texto transcrito abaixo pode-se ver a importância destas câmaras térmicas e onde é que elas podem ser aplicadas.



Figura 14 - Imagem térmica em escuridão total¹¹

“A geração de imagens térmicas não é nada de novo. Porém até recentemente, os custos a tornavam proibitiva, tornando as aplicações práticas fora do ambiente militar muito raras. Isto começou a mudar à medida que novos sensores, novos materiais e outras melhorias foram aumentando os volumes e tornando os preços mais razoáveis. As câmaras podem ser agora encontradas em vários tipos de negócios como, por exemplo, a indústria de aviões, a indústria de navios e de segurança e vigilância. A tecnologia é

¹¹Disponível em:

http://www.axis.com/files/whitepaper/wp_axis_thermal_cameras_br_40474_1009_lo.pdf

também utilizada em serviços públicos como combate a incêndio e aplicação da lei. Por fim ela já aparece em produtos para os consumidores, embora frequentemente de alto custo como em veículos de luxo.”¹²

2.1.2.5 A videovigilância aérea

Desde à vários anos que a vigilância aérea tem estado presente na sociedade, mas era inicialmente uma opção dispendiosa porque era necessário para além de uma aeronave o respetivo piloto e em alguns casos o operador do equipamento de videovigilância. Nos últimos anos têm havido um grande desenvolvimento de aeronaves não tripuladas e completamente autónomas que conseguem voar por rotas definidas e áreas definidas. Estes dispositivos são designados por *drones*, AONT (Aeronaves de Observação Não Tripuladas ou VANT (Veículo Aéreo Não Tripulado) e começam a ser amplamente utilizados na vigilância de eventos de grande dimensão como por exemplo os jogos de futebol, espetáculos de música, e outros eventos desportivos, casamentos.

Também começam a dar os primeiros passos na vigilância das florestas na prevenção de incêndios. Estes dispositivos começam a serem vistos como uma grande revolução na prevenção de incêndios, pois conseguem alcançar e vigiar locais que não são acessíveis por meios terrestres e como normalmente dispõem de um Sistema de Informação Geográfico (SIG) como por exemplo GPS é possível enviar as coordenadas do início do foco do local de incendio para as autoridades competentes tornando possível intervir muito mais cedo. Estes dispositivos são uma solução mais económica devido ao facto de consumirem menos combustível, e não têm necessidade de um piloto. Pode ser necessário um operador do equipamento mas são extremamente.

Na imagem abaixo pode-se ver uma imagem de um drone e um VANT da força nacional de segurança pública.



Figura 15 –Um drone¹³ e um VANT da polícia Portuguesa ¹⁴

¹² Disponível em:

http://www.axis.com/files/whitepaper/wp_axis_thermal_cameras_br_40474_1009_lo.pdf

¹³ Disponível em: <http://www.airdrone.be/wp-content/uploads/2014/04/viedoes-drone-belgique-copie.png>

¹⁴ Disponível em: <http://imagens9.publico.pt/imagens.aspx/841059?tp=UH&db=IMAGENS>

2.1.2.6 O Face tracking

Esta tecnologia ligada à videovigilância é uma das mais recentes e uma das que mais têm evoluído e recebido mais atenção nos últimos anos, porque permite a identificação e seguimento de um indivíduo à distância.

Estes novos sistemas permitem identificar pessoas mesmo quando eles estão no meio de uma multidão. Recorrendo por exemplo a uma foto de um indivíduo procurado pelas forças de segurança, que pode ser identificado quando for capturado o seu rosto por uma destas câmaras. Esta nova tecnologia parece saída de um filme de ficção científica, mas a realidade é que já existem estes sistemas que já se encontram no mercado e em pleno funcionamento. Um dos grandes produtores e desenvolvedores desta tecnologia é a empresa NEC.¹⁵

Pode-ver em baixo a transcrição de uma pequena notícia informativa que nos fala desta tecnologia.



Figura 16 - NeoFace Watch¹⁶

“Lisboa, 6 de julho de 2015 – A NEC¹⁷ Corporation (TSE: NEC 6701) anunciou o lançamento da mais recente edição do NEC NeoFace Watch. O NeoFace Watch consegue identificar pessoas de interesse a partir de vídeo CCTV em tempo real, de vídeo gravado, ou de imagens guardadas em bases de dados. Esta mais recente versão introduz melhorias significativas de desempenho, aumentando a velocidade de processamento de vídeo em tempo real para 30 imagens por segundo e a eficiência de interação com bases de dados de grandes dimensões. O NeoFace Watch pode ser integrado com os atuais sistemas de videovigilância para detetar correspondências entre as faces captadas

¹⁵Disponível em: http://www.nec.com/en/global/solutions/safety/face_recognition/NeoFaceWatch.html

¹⁶ Disponível em:
http://www.nec.com/en/global/solutions/safety/face_recognition/images/Face_Recognition_FR_Pic.png

¹⁷ Disponível em: www.nec.com

por esses sistemas e uma lista pré-configurada de indivíduos, visando despoletar alertas junto das forças de segurança.”¹⁸

A tecnologia de reconhecimento facial é uma tecnologia bastante controversa principalmente devido ao respeito pela privacidade das pessoas e pela sua liberdade, o que deu maior significado a frases como “big brother”, segundo Kevin W. Bowyer [Bowyer,2003].

Pode-se ver no texto a seguir a transcrição de outra notícia onde se refere a implementação deste tipo de tecnologia na vigilância de eventos de desportivos.

“After the American Super Bowl XXXV in Tampa, Florida in June 2001, a major controversy ensued. It became public that police had used video cameras equipped with facial recognition technology (“facecams”) to scan the faces of the 100,000 visitors to the Bowl in search of wanted criminals.”¹⁹

2.2 A videovigilância

A videovigilância representa o futuro da vigilância onde cada vez mais se deixa cair o modelo tradicional de um vigilante humano e embora não sendo totalmente substituível pelas novas tecnologias pode ser amplamente complementado por estas.

Os sistemas de videovigilância são cada vez mais evoluídos e independentes e que operam nas mais diversas situações e locais tendo diversas finalidades tais como controlo de fluxos de trânsito, vigilância de acessos de veículos, proteção do ambiente e do património cultural e a proteção de bens e pessoas. E cada vez mais estes sistemas são instalados conforme se pode ver pela transcrição do texto abaixo.

“O uso da videovigilância tem assumido finalidades essenciais como seja, o controlo dos fluxos de trânsito, a vigilância do acesso de veículos a zonas de circulação limitada (v.g., centros históricos das cidades) e das infrações das regras de circulação de 3 veículos automóveis, a proteção do ambiente e do património cultural, a proteção de pessoas e bens, ou a garantia de condições de segurança em meio laboral. A sua utilização é tão massiva que há dados extraordinários do Reino Unido que estimam que só em espaços públicos existem cerca de 2,5 milhões de câmaras para fins de segurança, sendo que a imagem de um britânico “médio” é capturada 300 vezes por dia, assim como em Nova

¹⁸ Disponível em: http://pt.nec.com/pt_PT/press/201507/20150706_01.html

¹⁹ Disponível em: http://www.utwente.nl/bms/wijsb/organization/brey/Publicaties_Brey/Brey_2004_Face-Recognition.pdf

lorque, em Manhattan, foram identificadas para o mesmo fim 2,397 câmaras.” [Coelho,2010]²⁰.

2.2.1 As câmaras de videovigilância

Analisaram-se várias câmaras de videovigilância que se encontram no mercado, mesmo existindo uma grande variedade, estas não se encontram ainda bem preparadas para serem utilizadas em locais remotos sem infraestruturas, uma vez que estas não integram todos os componentes necessários como *modem* de comunicação de dados e sistema de geração e gestão da energia elétrica.

É possível adquirir câmaras de vídeo e seus componentes para uma utilização em locais sem energia elétrica e sem rede *internet* cablada mas para tal é necessário comprar os diversos componentes (fonte de energia, controlador de carga) e montar o sistema no local que se pretende vigiar. Esta é uma solução dispendiosa e que normalmente carece da necessidade de um técnico especializado para proceder a montagem dos diversos componentes necessários ao funcionamento da câmara de videovigilância.

Analisaram-se várias câmaras tendo em conta os seguintes parâmetros:

- Fonte de alimentação;
- Meio de comunicação;
- Aspeto exterior (camuflagem);
- Local de instalação;
- Preço.

Ao analisar estes parâmetros concluímos que as câmaras de videovigilância usadas na captura de imagens e vídeos da vida selvagem são as que mais se aproximam dos nossos intentos, devido que estas são alimentadas a baterias, algumas têm *modem* de comunicação de dados e ainda têm o aspeto um pouco camuflado. Pode-se ver a seguir alguns exemplos destas câmaras e algumas das suas características.

A câmara LTL5210A (Figura 17) é uma câmara de vigilância tanto noturna como diurna, que pode ser utilizada em diversas situações:

- Observação de vida selvagem;
- Controlo de Coutadas;

²⁰ Disponível em:

<http://wiki.di.uminho.pt/twiki/pub/Education/Archive/InformaticaJuridicaT3/AvideovigilnciaeosoutrostratamentosdeimagemDadosPessoais.pdf>

- Vigilância de propriedades.



Figura 17 - Câmara LTL5210A²¹

A câmara LTL5210A é à prova de água podendo ser utilizada em espaços fechados e em espaços abertos. Tem uma qualidade de imagem de 12 Mega *pixels*, visão noturna, e sensor de movimento que permite tirar fotografias assim que o sensor incorporado na máquina seja ativado e que pode ser programado em função da distância a que se pretende a sua ativação. Permite tirar fotografias a cores durante o dia e a preto e branco durante a noite e possui leds de infravermelho que permitem a visão noturna num raio de 25 metros, a visão noturna ativa-se assim que deteta o anoitecer. Esta câmara têm um custo de 250 euros²².



Figura 18 - Spypoint Mini Live and Live 4G Wildlife Câmara²³.

A câmara Spypoint Mini Live and Live 4G Wildlife (Figura 18) permite enviar alertas através de mensagem ou *email*. Esta câmara envia as imagens e vídeos capturados para um servidor *Web* para que possam ser consultados e visualizados. Esta câmara pode ser

²¹Disponível em: http://image.basekit.com/live113847_ltl5210afront.jpg

²² Disponível em: http://oldboysoutdoors.com/obo-ltl-acorn-ltl-5210a/ltl-5210a_revised/

²³ Disponível em :<http://www.scottcountry.co.uk/images/large/live4g.jpg>

alimentada através de USB, fonte de alimentação de 12Vdc e têm entrada para painéis solares fotovoltaicos. Têm um custo de 677 euros²⁴.

A câmara UM565-3G MMS já têm a capacidade de enviar alertas por *sms*, *mms* ou *email* e pode gravar as imagens e vídeos na sua memória interna.

A sua alimentação é feita através de baterias embora também disponha de uma entrada para uma fonte de alimentação externa de 6Vdc. Esta câmara têm um custo de aproximadamente 485 euros²⁵.



Figura 19 – A Spypoint Mini Live and Live 4G Wildlife Câmara²⁶.

Embora estas câmaras de videovigilância estejam muito próximas do conceito aqui pretendido, verifica-se que existem ainda fatores em que podemos ser diferenciadores, principalmente nos seus aspetos exterior e na sua capacidade de camuflagem.

Se analisarmos as câmaras referidas anteriormente, verifica-se que o seu aspeto é muito identico mesmo tendo havido, em alguns casos alguma preocupação com a sua camuflagem.

Grande parte destas câmaras não dispõem de *modem* de comunicação de dados, guardando suas imagens e vídeos na sua memória física que depois podem ser descarregados e visualizados através de um computador. As câmaras que dispõem de *modem* de comunicação de dados, muitas das vezes só permitem enviar alertas ou imagens não permitindo a visualização de vídeo em tempo real (*streaming*).

²⁴ Disponível em: <http://www.scottcountry.co.uk/products-Spypoint-Mini-Live-and-Mini-Live-4G-Cellular-Wildlife-Camera-Trap-5797.htm>

²⁵ Disponível em: http://www.trailcameras.com.au/uovision_um565.htm

²⁶ Disponível em: http://www.trailcameras.com.au/index_htm_files/38661.jpg

2.2.2 Locais de implementação da videovigilância

Pretendemos fazer uma análise dos locais onde normalmente se implementam sistemas de videovigilância e identificam quais os objetivos da videovigilância nestes locais.

2.2.2.1 A videovigilância urbana

A videovigilância urbana visa trazer alguma tranquilidade as pessoas pois é um grande meio de prevenir ataques à integridade física das pessoas.

As câmaras de videovigilância em locais urbanos são uma realidade em todo o mundo e cada vez mais assumem um papel importante na sociedade devido a sua capacidade de dissuasão e prevenção de crimes.

Estes meios de vigilância têm sido reforçados nos locais já existentes e adotados a novos locais.

Em baixo são apresentados alguns excertos de algumas notícias que demonstram como a videovigilância está a ser fortemente implementada em cidades de todo o mundo nomeadamente em Portugal.

“A Câmara da Amadora prevê começar “ainda este ano” a instalar as 103 câmaras de videovigilância autorizadas para o concelho, para prevenir a criminalidade urbana, revelou à agência Lusa a presidente da autarquia.”²⁷



Figura 20 - Notícia sobre videovigilância urbana na Amadora²⁸.

²⁷ Disponível em: <http://www.ionline.pt/264973>

²⁸ Disponível em: http://www.ionline.pt/media/transferido/styles/625x350-imagem_interior/public/amadora_0.jpg?type=artigo

A cidade do Porto, é também uma das cidades que pretende implantar soluções de vigilância urbana sobretudo pelo facto de se ter tornado uma das cidades mais turística da Europa.

“Um despacho do Ministério da Administração Interna publicado hoje no Diário da República (DR) autoriza a instalação e a utilização de um sistema de videovigilância na Baixa do Porto, apesar do parecer negativo da comissão de proteção de dados.”²⁹

“As câmaras de videovigilância na Ribeira, Porto, vão voltar a ser ligadas. O Governo aprovou, esta quarta-feira, em Conselho de Ministros, as alterações legislativas que a Associação de Bares, promotora do sistema, reivindicava. As câmaras vão poder gravar 24 horas por dia e a autorização prolongar-se-á por dois anos (mais dois renováveis).”³⁰

Na figura abaixo pode-se ver uma câmara de videovigilância colocada na ribeira do porto para proceder a vigilância do espaço.

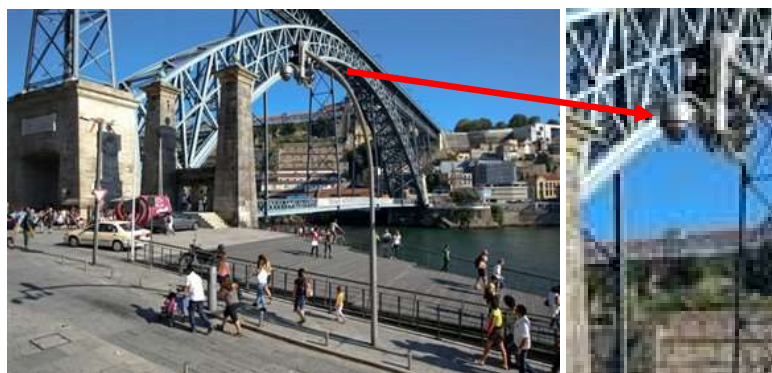


Figura 21 - Videovigilância na ribeira Porto ³¹

2.2.2.2 Videovigilância em espaços comerciais

A videovigilância em espaços comerciais é uma forma de reduzir as perdas e aumentar também o desempenho da loja.

Os sistemas de videovigilância já dispõem de inteligência e capacidade de detetar possíveis furtos e podem notificar as pessoas responsáveis pela loja. Mas também é

²⁹ Disponível em: <http://www.publico.pt/local/noticia/camara-do-porto-estuda-instalacao-de-videovigilancia-na-movida-da-baixa-1628786>

³⁰ Disponível em: http://www.dn.pt/inicio/portugal/interior.aspx?content_id=4262022

³¹ Disponível em: <http://www.dn.pt/storage/DN/2014/big/ng3734644.jpg?type=big&pos=0>

possível utilizar os sistemas de videovigilância para analisar *layout* de loja ou o comportamento dos funcionários.

Estes sistemas de videovigilância também começam a ser utilizados para contar o número de pessoas em loja e podem também analisar padrões de consumo dos clientes.



Figura 22 - Videovigilância em loja comercial ³²

2.2.2.3 A videovigilância de espaços especiais (aeroportos)

Os aeroportos são talvez dos espaços com mais regras restritas de segurança, devido a constatare presença de perigos nomeadamente a ameaça atos de terrorismo.

Tudo em um aeroporto ocorre em ritmo elevado o que leva a necessidades redobradas no que diz respeito na vigilância. As tecnologias de videovigilância estão continuamente a evoluir e a ajudar a tornar os aeroportos em lugares seguros, principalmente na ajuda da prevenção de atos de terrorismo conforme é do conhecimento de todos do perigo. O ato bárbaro do 11 de Setembro de 2001 nos USA em muito contribuiu para um reforço da videovigilância nestes espaços.

Os sistemas de videovigilância utilizados nos aeroportos são os mais avançados do mundo, pois utilizam sistemas avançados de processamento e análise de vídeo onde conseguem em tempo real detetar ações específicas, fazer reconhecimento facial e assim encontrar potenciais terroristas através de base de dados de pessoas identificadas pelas autoridades.

Estes sistemas de videovigilância utilizam a tecnologia de reconhecimento comportamental, onde as câmaras podem ser programados para detetar incidentes

³² Disponível em:

http://bambooinnovator.files.wordpress.com/2013/04/tech_shopping18__01__630x420.jpg?w=945&h=630

como objetos deixados, congestionamentos, movimentos inversos, e até os carros estacionados em locais impróprios por demasiado tempo.

Estes sistemas de videovigilância são pensados para ser flexíveis e escalonáveis conforme as necessidades dos aeroportos e seu crescimento.

Os sistemas de videovigilância nos aeroportos têm os seguintes propósitos operacionais e de segurança.

Propósitos operacionais:

- Fluxo e gestão de tráfego;
- Veículos mal estacionados;
- Fluxo de passageiros;
- Gerir as filas de espera;
- Gerir padrões de qualidade

Propósitos de segurança:

- Segurança Pública geral (pessoas e bens);
- Segurança dos funcionários;
- Proteção dos funcionários e passageiros de passagem;
- Observação do pessoal trabalhador (denúncias de comportamentos inadequados, agressões);
- Bagagens esquecidas;
- Prevenção e detecção de crimes;
- Apreensão e repressão de infratores;
- Evidências/provas para uso do sistema judicial.

Na Figura 23 pode-se ver um exemplo de uma câmara de videovigilância colocada em um aeroporto.

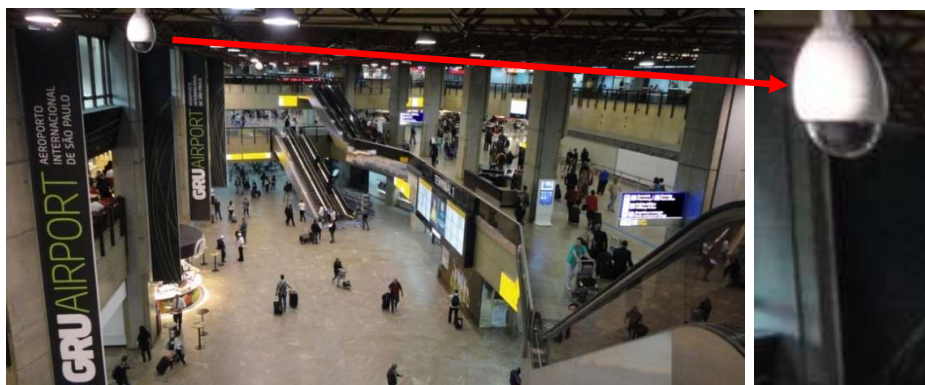


Figura 23 – Sistema de videovigilância para aeroportos ³³

2.2.2.4 A Videovigilância em autoestradas

Nas últimas décadas, têm sido dada uma especial atenção aos sistemas de inteligentes de transporte³⁴. O forte crescimento e desenvolvimento desta área têm-se dado devido à elevada urbanização bem como o aumento da densidade populacional e com isto a explosão do número de carros presentes nas estradas o que levou a necessidade do desenvolvimento de sistemas de videovigilância para estradas e autoestradas.

Estes sistemas de videovigilância são sistemas complexos que permitem analisar os movimentos de fluxo, bem como calcular a velocidade dos veículos, detetar a ocorrência de acidentes e mesmo tentar prever o acontecimento. Estes sistemas ajudam na redução substancial de acidentes, diminuição dos índices de poluição devido ao bom fluxo dos automóveis devido a boa gestão de frotas e veículos presentes nas estradas.

Proporcionam ainda intervenções mais rápidas em casos de acidentes.

Na Figura 24, pode-se ver um exemplo de um sistema de videovigilância que tem a capacidade de detetar acidentes e a velocidade dos veículos.

³³ Disponível em: <http://www.meusroteirosdeviagem.com/wp-content/uploads/2012/05/GRU-Airport-0003.jpg>

³⁴ Disponível em: <http://its.isr.uc.pt/publications/MScThesis-GMonteiro.pdf>

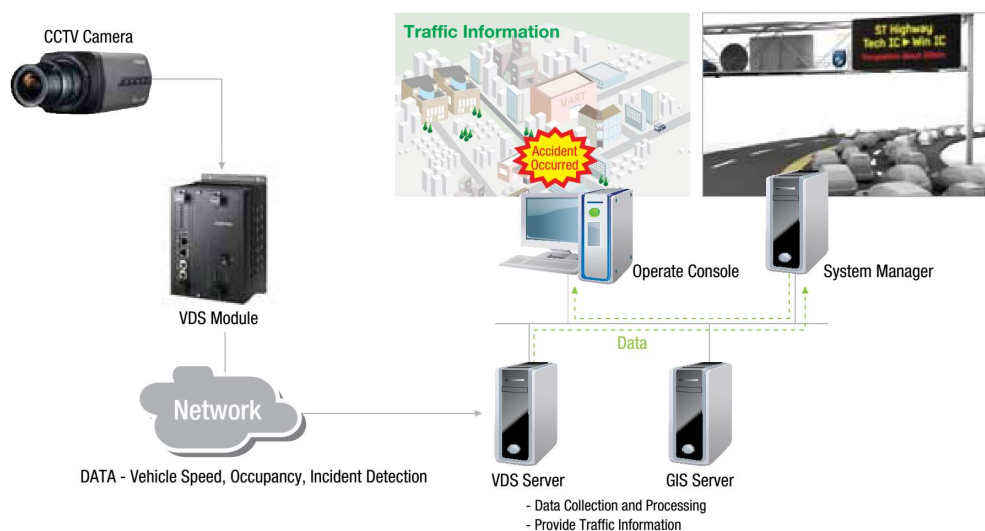


Figura 24 - Sistema de videovigilância em autoestradas³⁵

Estes sistemas de gestão de tráfego e fluxo para estradas são um grande passo tecnológico, devido ao número exponencial de câmaras colocadas nas estradas e autoestradas. Era praticamente impossível fazer a sua gestão unicamente com o recurso de operadores humanos.

2.2.2.5 A videovigilância em locais desportivos

Qualquer evento que envolva grandes multidões pode ser um alvo para a atividade criminal. Os eventos desportivos são um bom exemplo de locais onde a exigência para as forças de segurança são bastante elevadas para que seja possível manter as multidões sob controlo. Qualquer perturbação ou ameaça em grande escala deve poder ser sessada sem qualquer dano para as pessoas ou bens.

Os sistemas de videovigilância têm um papel fundamental nos recintos desportivos pois com eles é possível monitorizar a entrada e saída de pessoas e reencaminha-las para os locais de menor aderência.

Durante os eventos desportivos é comum as emoções estarem bastante ativas e surgirem locais de conflito. Com os sistemas de videovigilância é possível detetar estes focos de violência, distúrbios entre massas e fazer com que as forças de segurança intervenham mais rapidamente para acalmar os ânimos.

³⁵ Disponível em: http://www.samsungsecurity.com/_img/menu4/12_SISS_catalog_120328_E_F.pdf

Nestes eventos, por vezes os árbitros e jogadores são alvo de represálias sendo de violência. São lançados por vezes objetos, contra eles pelos espectadores que estão nas bancadas a assistir ao evento.

Os sistemas de videovigilância podem ser um fator de dissuasão destes atos mas também podem servir como prova judicial de que estes atos aconteceram e quem foi o autor dos mesmo e este ser levado à justiça como se pode ver pelo seguinte texto: *“As gravações obtidas por videovigilância podem ser meio de prova em tribunal desde que a Comissão de Dados autorize a instalação”*³⁶.

Estes locais de eventos desportivos, são alvos apetecíveis para proceder a atos de terrorismo, pelo que os sistemas de videovigilância podem ser utilizados no reconhecimento de potencial terroristas sendo que, em alguns destes locais, já foram utilizados sistemas de reconhecimento facial para detetar criminosos conhecidos pelas forças de segurança.

Na figura abaixo pode-se ver a imagem de um estádio desportivo com diversas câmaras de videovigilância.

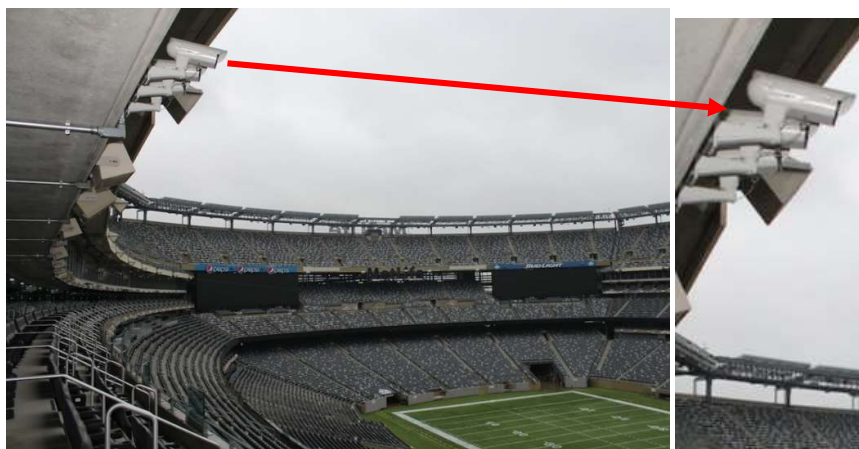


Figura 25 - Sistema de videovigilância de um estádio desportivo.

2.2.3 Enquadramento legal da videovigilância

Neste ponto pretendemos fazer o enquadramento da videovigilância no panorama jurídico nacional. Existem várias leis e decretos de Lei (DL), que regulamentam o uso e utilização de sistema de videovigilância em locais públicos de utilização comum e locais privados, que são as seguintes:

³⁶Disponível em: <http://www.inverbis.pt/2007-2011/tribunais/validade-imagens.html>

- Lei 34/ 2013 – utilização de sistemas de videovigilância pelos serviços de segurança privada e de autoproteção;
- Lei 1/ 2005 – regula a videovigilância pelas forças de segurança em locais públicos de utilização comum;
- Decreto-Lei 207/ 2005 - Regula os meios de vigilância Eletrónica rodoviária utilizados pelas forças de segurança;
- Lei 51/ 2006 – regula a utilização de sistemas de vigilância rodoviária pela EP e pelas concessionárias rodoviárias;
- Lei 33/ 2007 – regula a instalação e utilização de sistemas de videovigilância em táxis.

Em termos jurídicos quando nos referimos a sistemas de videovigilância, estamos a referir sistemas de controlo de vídeo constituídos por uma ou mais câmaras, que permitem a recolha de imagens e som de pessoas que circulam em determinado espaço. Neste projeto, de videovigilância enquadra-se na Lei 1/ 2005 que entretanto foi alterada e republicada para a Lei n.º 9/2012, que regula a utilização de câmaras de videovigilância pelas forças e serviços de segurança em locais públicos e de utilização comum, em que esta prevê a utilização de câmaras para proteção de instalações com interesse para a defesa e segurança, Proteção da segurança das pessoas e bens, públicos ou privados, e prevenção da prática de factos qualificados pela lei como crimes, em locais em que exista razoável risco da sua ocorrência, prevenção de atos terroristas, proteção florestal e deteção de incêndios florestais.

A seguinte lei diz-nos o seguinte:

- A instalação de câmaras fixas, nos termos da presente lei, está sujeita a autorização do membro do Governo que tutela a força ou serviço de segurança requerente.
- A decisão de autorização é precedida de parecer da Comissão Nacional de Proteção de Dados (CNPd), que se pronuncia sobre a conformidade do pedido face às necessidades de cumprimento das regras referentes à segurança do tratamento dos dados recolhidos, bem como acerca das medidas especiais de segurança a implementar adequadas a garantir os controlos de entrada nas instalações, dos suportes de dados, da inserção, da utilização, de acesso, da transmissão, da introdução e do transporte e, bem assim, do previsto no artigo 4.º, nos n.os 4 e 6 a 8 do artigo 7.º, e nos artigos 8.º a 10.º 3 — O parecer referido

no número anterior é emitido no prazo de 60 dias a contar da data de receção do pedido de autorização, prazo após o qual o parecer é considerado positivo.

- Nos locais objeto de vigilância com recurso a câmaras fixas é obrigatória a afixação, em local bem visível, de informação sobre as seguintes matérias: A existência e a localização das câmaras de vídeo, a finalidade da captação de imagens e sons, o responsável pelo tratamento dos dados recolhidos, perante quem os direitos de acesso e retificação podem ser exercidos.

3 O protótipo SVR - Sistema de Videovigilância Remota

“A pergunta idiota é o primeiro vislumbre de algum desenvolvimento totalmente novo.”

Alfred Whitehead

No presente capítulo apresenta-se o modelo conceptual do sistema de videovigilância (SVR- sistema de videovigilância remota), que se pretende que seja a solução para o problema identificado. Identificam-se os requisitos que são necessários cumprir no desenvolvimento do SVR bem como todas as tecnologias que serão necessárias à sua realização. Apresenta-se toda a descrição técnica do desenvolvimento do sistema de videovigilância SVR.

3.1 Introdução

Após a reflexão sobre o problema apresentado da vigilância em locais remotos e sem energia elétrica e das tecnologias e que existem atualmente, neste capítulo pretende-se apresentar a nossa solução para este problema. Pode-se ver o modelo conceptual da solução e quais as tecnologias que serão utilizadas e que requisitos serão necessários cumprir bem como todo o desenvolvimento até chegar ao final da solução.

Todos os trabalhos científicos têm a necessidade de seguir uma determinada, metodologia para atingir a resultados, esta dissertação de mestrado não foi exceção e como tal foi adotado a metodologia ADDIE para o desenvolvimento da mesma.

3.2 O modelo ADDIE

O modelo ADDIE consiste em cinco fases distintas: Análise, Design, Desenvolvimento, Implementação e Avaliação.

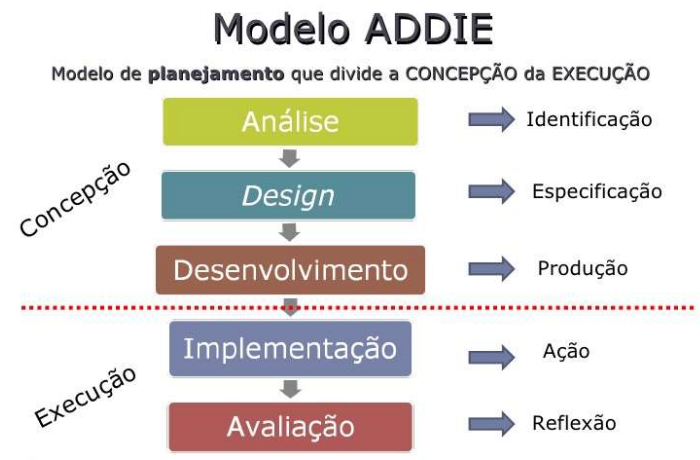


Figura 26 - Modelo ADDIE³⁷

Este modelo surgiu na década de 1950 e foi desenhado exclusivamente para o exército americano. Atualmente este modelo é amplamente utilizado em todo mundo como um guia para o *design* e gestão de projetos educacionais.

Esta metodologia assenta na premissa que se deve finalizar cada uma das etapas antes de passar para a próxima.

Em seguida temos a descrição de cada uma das etapas:

- **Análise**

Nesta etapa se definem todos os requisitos a seguir para a realização do projeto. Para definir os requisitos e objetivos do projeto é feito uma análise de mercado e um estudo de arte do que existe em relação ao tema do projeto.

Nesta fase foi feito o estudo do problema da vigilância em locais remotos sem infraestruturas de energia elétrica e rede internet.

Fez-se um estudo sobre a vigilância e as tecnologias de apoio para proceder a fase de desenho e assim apresentar um modelo conceptual de um sistema de solução ao problema identificado.

- **Desenho**

³⁷ Disponível em: <http://image.slidesharecdn.com/iniciativadedesigninstrucionalenumainstituioedeensinosuperior-091127113836-phpapp02/95/iniciativa-de-design-instrucional-em-uma-instituio-de-ensino-superior-7-728.jpg?cb=1259321963>

Nesta fase é feito o desenho conceptual do sistema onde se define a arquitetura e tecnologias a utilizar para concretizar todos os objetivos e cumprir com todos os requisitos.

É possível ver o modelo conceptual desenvolvido na fase de desenho no ponto 3.3 em que é possível verificar em que consiste o sistema que será a resposta ao problema apresentado no ponto 1.2.

- **Desenvolvimento**

A etapa do desenvolvimento é onde se materializa o projeto. Nesta fase é realizado o desenvolvimento do projeto utilizando as tecnologias e arquiteturas e tecnologias definidas na análise conceptual.

- **Implementação**

Nesta fase é feita uma verificação ao projeto e se verifica se é necessário alterar o mesmo. O projeto é testado, avaliado e realizam-se todas as alterações necessárias de forma a o melhorar constantemente até se chegar ao final do produto.

- **Avaliação**

Esta é a ultima fase do modelo ADDI, em que se procede a uma meticulosa avaliação do projeto em que se verifica se todos os requisitos foram cumpridos e os objetivos alcançados e qual o grau de satisfação por parte do utilizador ou cliente final em relação ao projeto/produto.

3.3 O modelo conceptual

Considerando que nos locais remotos não existe eletricidade, a sua vigilância ficaria naturalmente comprometida, uma vez que todos os sistemas existentes necessitam de uma fonte de alimentação elétrica.

Uma alternativa, poderia ser recorrer a baterias. No entanto, a sua capacidade é limitada o que obrigaria a uma intervenção humana permanente.

A evolução tecnológica evidenciada nos últimos anos proporciona atualmente meios capazes de autoalimentar energeticamente sistemas através de painéis fotovoltaicos.

Para além do problema da inexistência de energia elétrica nestes locais não existe rede cablada nem rede sem fios (Wi-fi, 802.11), para acesso à internet. Para contornar este problema o protótipo que propusemos é capaz de armazenar as imagens e vídeos no sua

memória interna e no caso de existir rede móvel é possível ligar à internet através desta e assim fazer o *streaming* de vídeo, enviar notificações e controlar o sistema à distância.

Para o modelo proposto definimos como principais requisitos a dimensão do protótipo (que deveria ser o mais reduzido possível para que seja pouco detetável) bem como:

- CPU ou computador (o mais pequeno possível)
- Uma câmara de vídeo
- Ligação à *Web*
- Autonomia de energia
- Sistema de armazenamento

SVR - Sistema de Vídeo-Vigilância Remota

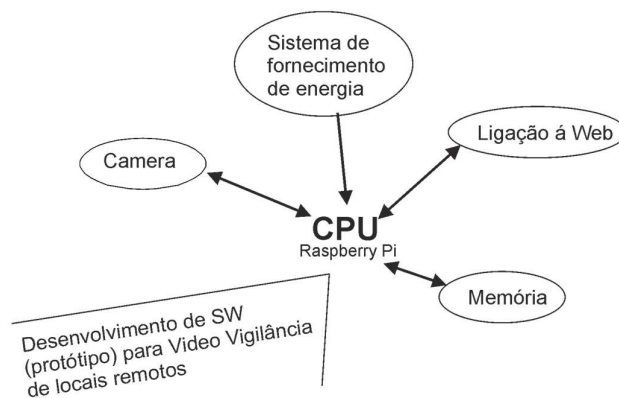


Figura 27 - O modelo conceptual do SVR

Conforme se pode ver na Figura 27, a juntar aos componentes de *hardware* identificados para o sistema protótipo denominado Sistema de Vigilância Remota (SVR) teria de ser desenvolvido um mecanismo (*software*) capaz de detetar a intrusão e que pudesse guardar uma ou várias imagens ou vídeos da ocorrência em cartão de memória ou mesmo, através de uma ligação remota via GPRS, 3G ou 4G, enviar estes conteúdos para o computador do utilizador.

3.4 Levantamento de requisitos e casos de uso

De todas as tarefas que compõem o desenvolvimento de um projeto, o levantamento dos requisitos para a sua elaboração será das mais importantes e das que carecem mais atenção e dedicação. Face a essa importância, segue-se dois subcapítulos reservados a este tema, apresentando-se o processo levado a cabo na definição de todos os requisitos do sistema.

Os requisitos do sistema foram divididos em duas categorias, requisitos não funcionais e requisitos funcionais, estes serão apresentados nos pontos 3.4.1 e 3.4.2.

3.4.1 Levantamento de requisitos não funcionais

Os requisitos não-funcionais são aqueles que afetam a aplicação em termos de desempenho, segurança, usabilidade, entre outros. Estes requisitos influenciam os requisitos funcionais, através de restrições e adicionam valor e qualidade à aplicação.

3.4.1.1 O desempenho

Uma das premissas do projeto é que o desempenho, tanto dos serviços como da página *Web*, não comprometa a experiência do utilizador no momento da sua utilização. O utilizador final pretende utilizar serviços rápidos e cómodos, dado que todos os serviços disponibilizados dependem da conexão com a internet para efetuar a troca de informação, o desempenho é influenciado pela qualidade da mesma.

O serviço mais preponderante na performance da câmara de videovigilância é o servidor de vídeo. Este deve responder aos pedidos de informação, de forma eficaz e eficiente.

3.4.1.2 A parametrizabilidade

O sistema de videovigilância SVR deve permitir diversas parametrizações como alterar o *email* de notificações e configurar as diversas opções do servidor.

Para efetuar as diversas parametrizações o SVR dispõe na página *Web* de uma opção de alterar o *email* de notificação bem como uma hiperligação para uma página de configuração do servidor onde é possível configurar as diversas parametrizações do mesmo, como tamanho da imagem capturada, local de armazenamento em disco, taxa de captação de imagens, configuração de eventos em que se pode definir as ações que cada evento ativa.

3.4.1.3 A usabilidade

Existem diferentes definições de usabilidade, criadas por vários autores. Algumas delas são:

- [Rubin,1994]: “Um conjunto de quatro fatores reunidos em um dispositivo: 1) capacidade de ser usado com sucesso; 2) facilidade de ser usado; 3) capacidade de o usuário aprender a usar o dispositivo de forma simples e rápida; 4) Provocar satisfação visual ao usuário”;

- [Nielsen,1993]: “Um conjunto de propriedades de uma interface que reúne os seguintes atributos: 1) Fácil aprendizado; 2) Eficiência; 3) Capacidade de memorização; 4) Baixo índice de erros; 5) Satisfação e prazer ao uso”;
- [Preece, Rogers e Sharp ,2002]: “Fator que assegura que os produtos sejam fáceis de usar, eficientes

Pretende-se que a câmara de videovigilância (SVR) seja de fácil utilização. Que o utilizador compreenda intuitivamente como navegar na página *Web* e usufrua de todas as funcionalidades da câmara. E que a sua montagem e colocação em funcionamento seja de igual modo intuitiva.

3.4.1.4 A confiabilidade

Segundo Paula Prata confiabilidade indica a qualidade de serviço fornecido por um dado sistema e a confiança que justificadamente pode ser depositada nesse serviço [Prata,2007].

O SVR está dependente de serviços e como tal, devem possuir mecanismos de controlo a falhas, nomeadamente no acesso à internet, resposta dos serviços ou apresentação de informação inconsistente. Desta forma, no caso de existirem falhas, dependendo de qual se tratar é importante garantir a contínua execução, quando não for possível têm que ser capaz de recuperar e voltar a funcionar corretamente.

3.4.1.5 A segurança

Um dos aspetos mais importantes que se esperam em sistemas desta natureza é a segurança dos dados. A plataforma deve ser capaz de efetuar a autenticação do utilizador e a base de dados deve estar protegida contra terceiros.

A proteção de dados neste tipo de sistemas é de máxima importância pois é necessário salvaguardar o direito à privacidade.

Um sistema para ser seguro deve garantir três requisitos:

- Disponibilidade - Os serviços/recursos estão disponíveis sempre que necessários;
- Confidencialidade- A informação só está disponível para aqueles devidamente autorizados;
- Integridade- A informação não é destruída nem corrompida e o sistema têm um desempenho correto.

Pretende-se que o nosso sistema de videovigilância SVR seja capaz de manter todos os dados (vídeos e imagens) gravados em memória com integridade durante o período

desejado pelo utilizador e que estes estejam protegidos do acesso de pessoas alheias ao sistema para que não seja possível consultar esses dados nem destruí-los.

3.4.2 Levantamento de requisitos funcionais

Nos requisitos funcionais são descritas as principais funcionalidades que o sistema deve disponibilizar. Correspondem, portanto, aos requisitos básicos propostos no projeto. Por outras palavras, representam aquilo que o utilizador espera que o sistema ofereça, atendendo aos propósitos para qual o sistema é desenvolvido.

As funcionalidades a seguir descritas, foram continuamente analisadas e refinadas em diversas reuniões de acompanhamento com o orientador, com o objetivo de decidir o comportamento que o sistema deveria apresentar, que informação seria exposta e possível de gerir pelo utilizador.

As principais funcionalidades oferecidas ao utilizador são as seguintes:

- Registo de *email* de notificações;
- Ver o vídeo em tempo real;
- Descarregar as últimas gravações em que foi detetado movimento.

3.4.3 Casos de uso

Neste subcapítulo é apresentado o diagrama de caso de uso do protótipo. Após o levantamento de requisitos, é necessário elaborar uma representação da informação de forma mais detalhada e técnica, apresentando o comportamento do sistema e a interação do utilizador com o mesmo.

No diagrama de caso de uso que se segue é apresentado as funcionalidades do sistema, para uma melhor compreensão das características do protótipo desenvolvido.

3.4.3.1 O ator do sistema

A câmara tem unicamente um ator do sistema que é o próprio utilizador a interagir com a câmara de videovigilância e os seus serviços e funcionalidades.

3.4.3.2 O diagrama de caso de uso “Geral”

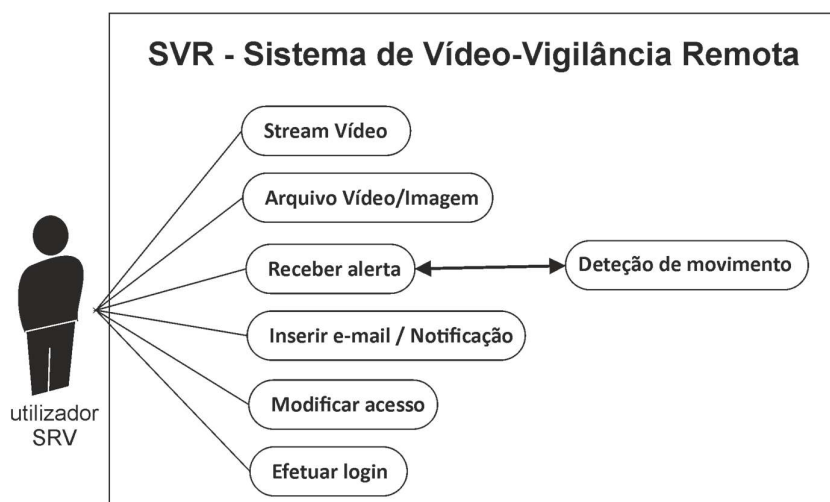


Figura 28 - Diagrama de caso de uso da camera de video-vigilância

Descrição dos casos de uso	
Ver <i>stream</i> vídeo	Permite ao utilizador ver o vídeo em <i>streaming</i> .
Arquivo imagem/vídeo	O utilizador pode descarregar o vídeo e imagens de quando foi detetado movimento.
Receber alerta	O sistema envia alerta para o utilizador quando houver deteção de movimento.
Inserir <i>email</i> de notificações	Esta opção permite ao utilizador inserir o <i>email</i> que vai receber as notificações quando houver deteção de movimento.
Modificar acesso	Possibilidade de modificar o acesso à página da câmara de videovigilância.
Efetuar login	Função de autenticação do utilizador.

Tabela 1 - Descrição de casos de uso

3.4.3.3 O diagrama de sequência de autenticação e download arquivo

Apresentado o diagrama de caso de uso da câmara de videovigilância pode-se ver o diagrama de sequência do processo de autenticação e descarregamento do arquivo de imagens e vídeos.

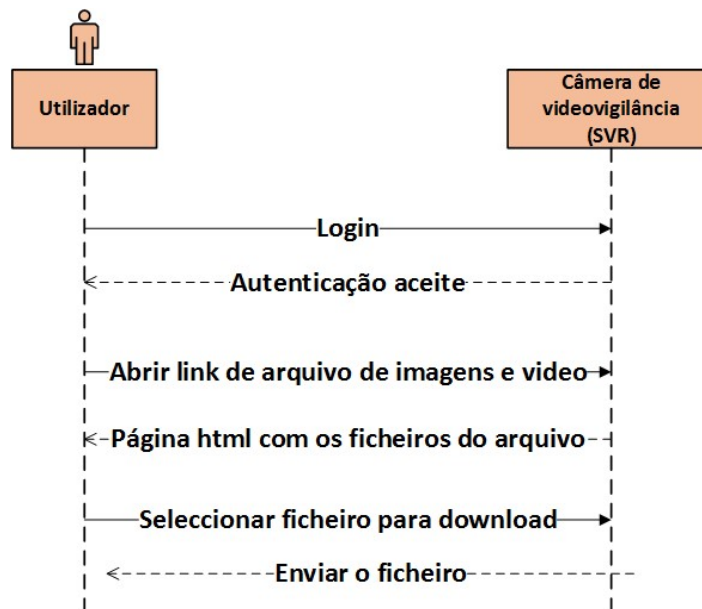


Figura 29 - Diagrama de sequencia de autenticação e download arquivo

Na figura acima pode-se ver o diagrama de sequência do processo de autenticação e visualização dos ficheiros e vídeos gravados na memória do protótipo SVR.

3.5 Análise de recursos e tecnologias

Neste subcapítulo, serão abordadas diferentes tecnologias, que serão utilizadas no desenvolvimento do projeto sejam elas *software* ou *hardware*. Esta descrição de tecnologias permite escolher quais as melhores para dar resposta a todos os requisitos e objetivos do projeto.

3.5.1 O linux Raspbian

Raspbian³⁸ é um sistema operativo baseado em *Debian* que foi otimizado para correr na placa de desenvolvimento Raspberry Pi. O Raspbian é mais que um sistema operativo, este vem com mais de 35000 pacotes de *software* pré-compilado de fácil instalação no Raspberry Pi.

³⁸Disponível em: <https://www.raspbian.org>

3.5.2 O Apache2 Web Server

O Apache é um servidor *Web* livre, o projeto é gerido em conjunto por um grupo de voluntários espalhados pelo mundo, usando a Internet e a *Web* para se comunicar, planejar e desenvolver o servidor e a sua respetiva documentação.

Devido à sua versatilidade, possibilidade de configuração e mesmo à compatibilidade com diversas linguagens de programação foi determinado o uso deste para disponibilizar a página *Web* com o respetivos serviços disponibilizados ao utilizador final.

Apache disponibiliza para instalação, diversas bibliotecas públicas de *add-ons*, é um projeto bem documentado e no caso de existir alguma dificuldade ou problema é possível, com enorme facilidade, encontrar uma solução na sua enorme comunidade. É também muito conhecido na comunidade do Raspberry Pi.

De acordo com a página *Web* W3Techs, Apache tem cerca de 60% de quota de mercado referente a servidores *Web*. Com este resultado é o mais utilizado para *Websites*.

3.5.3 O Servidor Motion

*Motion*³⁹ é um servidor de *streaming*, que monitoriza o sinal de vídeo de diferentes câmaras e têm a capacidade de detetar se uma parte significativa das imagens sofreram alterações, ou seja, este é capaz de detetar movimento.

Este servidor é escrito em linguagem C e pode ser completamente configurado e utilizado utilizando a linha de comandos ou então utilizando scripts de configuração. O servidor *Motion* utiliza como formatos de saída *JPG*, *PPM*, *MPEG Vídeo Sequences*.

3.5.4 O servidor de FTP Vsftpd

Vsftpd⁴⁰ é um servidor de FTP para sistemas Unix, Linux. É seguro e extremamente rápido. Este servidor de FTP é capaz de lidar e implementar configurações bastante mais complexas, tais como:

- Virtual IP configurations;
- Virtual users;
- Standalone or inetd operation;

³⁹ Disponível em: <http://www.lavrsen.dk/foswiki/bin/view/Motion/WebcamServer>

⁴⁰ Disponível em: <https://security.appspot.com/vsftpd.html>

- Powerful per-user configurability;
- Bandwidth throttling;
- Per-source-IP configurability;
- Per-source-IP limits;
- IPv6;
- Encryption support through SSL integration.

Este servidor de FTP ocupa pouco espaço é bastante modular e recomendado para quem necessita de um servidor de FTP seguro, elevado desempenho e estabilidade.

3.5.5 A linguagem de programação PHP

A “PHP: Hypertext Preprocessor”⁴¹ é uma linguagem de programação executada do lado do servidor. Desde o seu nascimento tem vindo a dar suporte às necessidades dos programadores e, conseqüentemente, evoluindo: desde a versão 1.0 até à última versão 5.5, com data de 20 de Junho de 2014. A evolução da linguagem de programação, tem ocorrido de forma natural, devido às linguagens de programações concorrentes, às exigências das *frameworks* como é o caso da *Zend Framework*, *Cake PHP*, *Symfony2*, entre outras, e obviamente devido às exigências do mercado.

A linguagem PHP, é uma linguagem de programação bastante ativa, isto é, no lançamento de uma nova versão são corrigidos bugs a nível de segurança, erros ou mesmo performance. A versão instalada no servidor Apache é a PHP 5.5.9, é considerada a mais recente e estável.

Prevaleceu o uso desta linguagem de programação, uma vez que é atual e bastante utilizada devido às suas diversas características: portabilidade, *frameworks* robustas, capacidade de interagir com diversa base de dados. Também a familiaridade com esta linguagem e o enorme suporte oferecido pela comunidade PHP foram fatores que pesaram nesta escolha. Esta linguagem de programação foi usada no desenvolvimento do acesso à base de dados *Mysql*.

⁴¹ Disponível em: <http://php.net/>

3.5.6 A linguagem HTML

O *HTML* (Hypertext Markup Language) é a linguagem de marcação padrão, usada para criar páginas *Web*. Os navegadores *Web* conhecidos por *browsers* têm a capacidade de ler os ficheiros *HTML* enviados pelo servidor *Web* e interpreta-los e apresentar a própria informação contida no ficheiro sem as tags *HTML*, mas utiliza-as para interpretar e formatar o conteúdo da página. Os ficheiros *HTML* têm extensão. *html* ou *.html*. Neste momento a versão mais recente do *HTML* é denominada de *HTML5* e com esta é possível desenvolver aplicações mais dinâmicas com recursos a multimédia sem a necessidade de *plugins* ou tecnologias como o *Flash*.

Esta linguagem junto com outras tecnologias como *CSS*, *PHP*, *MYSQL*, e *BOOTSTRAP* serão utilizadas na construção da página *Web* da câmara de videovigilância SVR.

3.5.7 O CSS

O *Cascading Style Sheets* (*CSS*) é utilizado para especificar a aparência e a formatação de um documento *HTML*. O seu principal benefício é promover a separação entre a formatação e o conteúdo de um documento. No enquadramento do *HTML5* e do *JavaScript*, o *CSS* não é um elemento indispensável, isto é, podem ser implementadas funcionalidades *HTML5* e *JavaScript* sem recorrer ao *CSS*. No entanto, o *CSS* permite apresentar estas funcionalidades de forma mais agradável ao utilizador. Adicionalmente, facilita a mudança do estilo de apresentação e reduz o tamanho dos ficheiros *html*, já que os elementos relativos à apresentação são movidos do ficheiro. *html* para um ficheiro. *css*.

3.5.8 O Mysql

O *MySQL*⁴² é um servidor e gestor de base de dados (SGBD) relacionais *Open Source* com mais popularidade em todo o mundo. Esta concorre diretamente com base de dados de código fechado como *SQL Server* (Microsoft⁴³) e *Oracle*⁴⁴.

“O *MySQL* teve origem quando os desenvolvedores David Axmark, Allan Larsson e Michael “Monty” Widenius, na década de 90, precisaram de uma interface *SQL*

⁴² Disponível em: <https://www.mysql.com>

⁴³ Disponível em: <https://www.microsoft.com>

⁴⁴ Disponível em: <https://www.oracle.com>

compatível com as rotinas ISAM que utilizavam em suas aplicações e tabelas. Em um primeiro momento, tentaram utilizar a API *mSQL*, contudo a API não era tão rápida quanto eles precisavam, pois utilizavam rotinas de baixo nível (mais rápidas que rotinas normais). Utilizando a API do *mSQL*, escreveram em C e C++ uma nova API que deu origem ao *MySQL*.⁴⁵[Milani,2007].

O *MySQL*, têm a característica de ser bastante rápido, confiável, escalável e fácil de usar. Este tipo de base de dados é utilizado em aplicações desde e-commerce, transações *online* e aplicações embebidas.

3.5.9 A linguagem de programação Python

O *Python*⁴⁶, é uma linguagem de programação de fácil aprendizagem de elevado desempenho. É uma linguagem orientada a objetos e funciona de forma interpretada, o que a torna uma linguagem de desenvolvimento indicada para realizar scripts.

O interpretador de *python* e sua extensa biblioteca está disponível gratuitamente para diferentes plataformas na forma de código fonte ou em formato ficheiro binário.

Esta linguagem, tem imensas fontes de consulta *online* e milhares de utilizadores em todo o mundo o que permite obter suporte com grande facilidade.

3.5.10 O Bootstrap

O *Bootstrap*⁴⁷ é uma *framework* desenvolvida pelo *Twitter* para a criação de *front-ends* de forma simples e célere. Esta *framework* é constituída por um conjunto específico de ficheiros *CSS*, *HTML* e *JavaScript*, que utilizam uma série de padrões e/ou convenções para formulários, botões e tabelas. Permite então que um programador *Web* construa *front-ends* sofisticados e com *responsive design*, oferecendo uma ótima experiência de visualização, navegação, fácil leitura e redimensionamento para uma vasta gama de dispositivos. Deste modo, é possível dar mais enfoque a questões de usabilidade e apresentar facilmente *designs* apelativos, bem desenvolvidos e funcionais.

Com recurso a esta *framework* foi então possível desenvolver uma página *Web* com um interface agradável e de uma forma mais célere.

⁴⁵ Disponível em: <http://www.novateceditora.com.br/livros/mysqlcompleto/capitulo8575221035.pdf>

⁴⁶ Disponível em: <https://www.python.org/>

⁴⁷ Disponível em: <http://getbootstrap.com/>

3.5.11 O Raspberry Pi

O *Raspberry Pi* é um computador do tamanho de um cartão de crédito que se pode ligar a um monitor de computador ou televisão e que também permite ligar um rato e teclado. Pode-se utilizar este pequeno computador para fazer praticamente tudo que se espera de um desktop tal como, programar, utilizar processadores de texto e aceder à internet. Este pequeno computador também pode ser utilizado como um dispositivo de mais baixo nível e adicionar diversos componentes de *hardware*, como sensores e atuadores ligados a diversos tipos de interfaces de comunicação tais como: *UART*, *I2C*, *SPI*.

Este dispositivo de *hardware* é utilizado em larga escala por engenheiros e técnicos de eletrónica como placa de desenvolvimento para os mais diversos projetos e ideias inovadoras na área do *software* e *hardware*. Para se ter uma noção desde 2012 já foram vendidas mais de 5 milhões de unidades⁴⁸, tornando-se em umas das placas de desenvolvimento mais vendidas.

Um dos principais fatores de sucesso é este funcionar com *software* inteiramente livre, não sendo necessário o pagamento de qualquer licença.

O *Raspberry Pi* têm as seguintes características de *hardware*:

- A 900MHz quad-core ARM Cortex-A7 CPU;
- 1GB RAM;
- 4 Portas USB;
- 40 GPIO pins;
- Porta HDMI;
- Porta Ethernet;
- Jack combinado de áudio e vídeo de 3.5mm;
- Interface para câmara (CSI);
- Interface para ecrã (DSI);
- Micro SD card slot;
- VideoCore IV 3D graphics core.

Na Figura 30, pode-se ver um *Raspberry Pi* e a localização dos seus principais componentes.

⁴⁸Disponível em: <https://www.raspberrypi.org/blog/five-million-sold/>

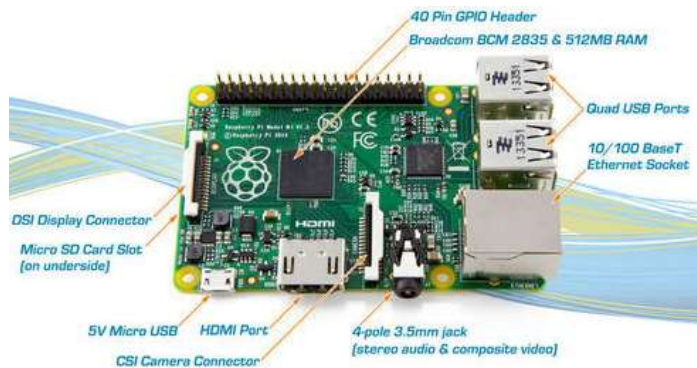


Figura 30 - Raspberry Pi versão 2.0⁴⁹

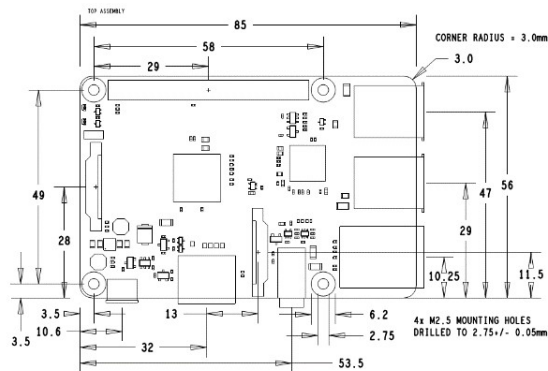


Figura 31 - Dimensões do Raspberry Pi 2.0⁵⁰

O *Raspberry Pi* têm dimensões bastante reduzidas para os periféricos que ele dispõe, pode-se ver as dimensões em milímetros (mm) na Figura 31. Sendo as dimensões outro dos fatores que contribui para o seu sucesso a nível mundial.

3.5.12 Os Painéis fotovoltaicos

Os painéis fotovoltaicos são constituídos por células fotovoltaicas ou solares que são responsáveis pela transformação da energia solar em energia elétrica, estes utilizam as propriedades dos materiais semicondutores (silício, Germânio). Quando devidamente dopados com elementos químicos como o Boro e o Fósforo, formam uma junção designada por P-N, num lado concentram-se cargas positivas e no outro, as cargas

⁴⁹ Disponível em: <http://i.stack.imgur.com/LctVT.jpg>

⁵⁰ Disponível em: <https://www.raspberrypi.org/documentation/hardware/raspberrypi/mechanical/Raspberry-Pi-Plus-V1.2-Mechanical-Drawing.pdf>

negativas, criando um campo elétrico permanente, que dificulta a passagem de eletrões de um lado para o outro. Quando um fóton incide com energia suficiente para excitar um eletrão, haverá circulação de corrente elétrica, gerando energia em corrente contínua, constituindo assim o chamado o efeito Fotovoltaico.

Uma célula fotovoltaica produz apenas uma tensão de aproximadamente de 0,4 V no seu ponto de máxima potência, sendo necessário a ligação de várias células em série e paralelo para se obter tensões e correntes mais elevadas.

3.5.13 O controlador de carga

O controlador de carga é o sistema de controlo do carregamento da bateria, de acordo com o seu tipo, para que esta seja totalmente carregada conforme o perfil indicado e para que esta possa atingir sua capacidade máxima como também maximizar o seu tempo de vida.

A carga é realizada com controlo de tensão e corrente, de acordo com a fonte de energia, podendo ser a partir de painel fotovoltaico ou fonte de alimentação contínua de baixa tensão.

3.5.14 O conversor de tensão

O conversor de tensão é um sistema que permite converter a tensão aos terminais da bateria no nível de tensão desejado para o circuito que está a montante desta.

Estes conversores de tensão podem ter várias topologias, conforme a necessidade ser de elevar ou baixar o nível de tensão que será disponibilizada ao circuito. Neste projeto serão vários circuitos, equipamentos ligados a montante do conversor de tensão estes são os seguintes:

- *Raspberry Pi*;
- *Modem* de dados;
- Câmara de vídeo.

3.6 Descrição técnica

Este capítulo aborda, detalhadamente, a solução final conseguida, com especial ênfase no aspeto técnico da solução e dos vários elementos que a compõem. Encontra-se dividido em várias secções para apresentar uma estrutura mais organizada.

Primeiramente é feita uma breve introdução ao sistema desenvolvido e posteriormente, será apresentada a instalação dos diferentes componentes de *software* necessários ao funcionamento, bem como o desenvolvimento de vários scripts de configuração do servidor de vídeo, para que este cumpra todos os requisitos que foram definidos na análise de requisitos.

3.6.1 Visão geral do sistema

O protótipo de videovigilância (SVR) foi desenvolvido de raiz, para tal foi necessário escolher todos os componentes de *hardware* e *software* necessários integrar para materializar numa solução funcional que cumpra todos os objetivos propostos.

A câmara de videovigilância é composta por diversos pacotes de *software* e serviços tais como servidor *FTP*, servidor de *streaming*, servidor *Web*, página *Web*, *scripts* de configuração, *scripts* de ações, interpretadores/compiladores de diversas linguagens (*PHP*, *Python*).

O *hardware* é construído por diversos componentes tais como minicomputador (*Raspberry Pi*), câmara de vídeo, controlador de carga, painéis solares, conversor de tensão DC/DC topologia STEP-UP.

Todos estes componentes de *software/hardware* são integrados de forma a criar um protótipo de videovigilância. Para tornar este em um produto comercial é necessário o desenvolvimento de uma caixa/estrutura que tenha o aspeto de um objeto existente na natureza como por exemplo uma rocha de forma a o tornar o mais camuflado possível, devido ao fim que se destina que é a vigilância de locais remotos e predominantemente rurais.

3.6.2 Diagrama do sistema

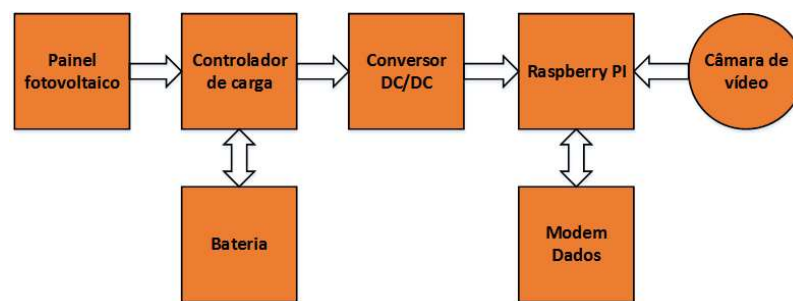


Figura 32 - Diagrama do Sistema de Videovigilância

3.6.3 Estudo do servidor de stream Motion

O servidor *Motion*⁵¹ é um servidor de *streaming*, que monitoriza o sinal de vídeo de diferentes câmaras e têm a capacidade de detetar movimento.

Este servidor é escrito em linguagem C e pode ser completamente configurado utilizando a linha de comandos ou então utilizando *scripts* de configuração. O servidor *Motion* utiliza como formatos de saída *JPG, PPM, MPEG Video Sequences*.

O servidor *Motion* é um projeto *Open Source*, sem qualquer custo associado, pois foi publicado sobre uma licença GNU GPL⁵². Isto significa que pode ser feito o *download* e a instalação do programa sem qualquer tipo de custo associado.

Os recursos disponíveis no servidor *Motion* são os seguintes:

- Tirar fotografias ao movimento detetado;
- Visualizar diferentes dispositivos de vídeo ao mesmo tempo;
- *Stream* em tempo real de uma câmara (utiliza *multipart/x-mixed-replace*)
- Criação de vídeo em tempo real através da utilização da biblioteca do *FFMPEG*;
- Possibilidade de tirar fotografias com uma cadência definida.
- Tirar fotografias utilizando o programa de agendamento *Cron*;
- Execução de programas externos sempre que for detetado movimento
- Execução de um programa externo específico no início de uma série de detecções de movimento.
- Execução de um programa externo no fim da detecção de movimento;
- Executar um programa externo sempre que é gravada uma imagem;
- Execução de programa externo sempre que é iniciado a criação de um vídeo;
- Execução de um programa externo quando é terminado a criação de vídeo;
- Seguidor de momento;
- Alimentação de base de dados *Mysql* ou *PostgreSQL* com os eventos que aconteceram;
- Possibilidade de usar outros interfaces *Web* de controlo como *motion.cgi*, *Kenneths Webcam Package*, *Kevins Webpage*, *X-Motion*;
- Controlo do Servidor através de um interface *Web*;
- Controlo automático de ruído e *threshold*;

⁵¹Disponível em: <http://www.lavrsen.dk/foswiki/bin/view/Motion/WebcamServer>

⁵²Disponível em: <https://www.gnu.org/licenses/gpl-2.0.html>

- Configuração do texto apresentado nas imagens;
- Configuração do nome com que são guardados os vídeos e as imagens.

O servidor *Motion* utiliza um ficheiro de configuração em que neste é possível configurar todos os parâmetros do servidor.

Alguns dos parâmetros que são possíveis configurar são os seguintes:

- *Webcam_maxrate* ;
- *Webcam_quality*;
- *Webcam_limit*;
- *Webcam_localhost*.

Os parâmetros *Webcam_maxrate* , *Webcam_quality*, são bastante importantes pois estão diretamente ligados à quantidade de tráfego que vai ser necessário transmitir pelo *modem* de dados, quanto maior a qualidade maior a largura de banda necessária para transmitir o vídeo.

O parâmetro *Webcam_localhost* é um parâmetro em que se pode limitar a utilização da câmara unicamente a redes locais, o que no nosso caso a câmara tem de estar disponível para fora da rede local para que seja possível ver o vídeo em qualquer parte do mundo desde que exista ligação à internet.

Parametrizações	Valor	Descrição
Webcam_port	valores: 0 - 65535	Porta para qual é enviado o <i>stream</i> de vídeo
	Por defeito: 0 (desligado)	
threshold	Valores: 1 - 2147483647	Definição de valor para qual começa a ser detetado movimento.
	Por defeito: 1500	
control_port	Valores: 0 - 65535	Porta de acesso à página de configuração
	Por defeito: 0 (desligado)	
daemon	Valores: on, off	Permite iniciar o servidor no arranque sem bloquear a consola
	Por defeito: off	
framerate	Valores: 2 - 100	Numero de <i>frames</i> por segundo
	Por defeito: 100 (no limite)	
height	Valores: Depende do dispositivo	Altura em pixéis.
	Por defeito: 288	
jpeg_filename	Valores: 4095 caracteres máximo	Nome das imagens
	Por defeito: %v-%Y%m%d%H%M%S-%q	

movie_filename	Por defeito: %v-%Y%m%d%H%M%S	Nome dos vídeos
width	Valores: Depende do dispositivo	Largura em pixéis
	Por defeito: 352	
rotate	Valores: 0, 90, 180, 270	Rotação do vídeo
	Por defeito: 0 (Sem rotação)	

Tabela 2 - Tabela de parametrizações do servidor

Na Tabela 2, pode-se ver algumas das configurações mais importantes, quais os valores de entrada e qual sua função.

Para além de todos os parâmetros configuráveis o servidor *Motion* dispõe também de uma lista de eventos que podem desencadear ações, os eventos são os seguintes:

Eventos	Valores	Descrição
on_area_detected	Valores: 4095 (máximo de caracteres)	Evento gerado quando detetado uma variação na área definida para o algoritmo de deteção.
	Por defeito: Não definido	
on_camera_lost	Valores: 4095 (máximo de caracteres)	Evento gerado quando perdida a comunicação com a câmara.
	Por defeito: Não definido	
on_event_end	Valores: 4095 (máximo de caracteres)	Evento gerado no fim da deteção de movimento.
	Por defeito: Não definido	
on_event_start	Valores: 4095 (máximo de caracteres)	Evento gerado passado algum tempo de ter sido detetado movimento.
	Por defeito: Não definido	
on_motion_detected	Valores: 4095 (máximo de caracteres)	Evento gerado quando detetado um <i>frame</i> diferente.
	Por defeito: Não definido	
on_movie_end	Valores: 4095 (máximo de caracteres)	Evento gerado quando é concluída a utilização do <i>ffmpeg</i>
	Por defeito: Não definido	
on_movie_start	Valores: 4095 (máximo de caracteres)	Evento gerado quando é criado um vídeo.
	Por defeito: Não definido	
on_picture_save	Valores: 4095 (máximo de caracteres)	Evento gerado quando uma imagem é gravada.
	Por defeito: Não definido	

Tabela 3 - Tabela de eventos do servidor

O servidor *Motion* aceita diversos especificadores para serem utilizados em opções de texto e nomes de ficheiros. Em anexo neste documento podem-se ver todos os especificadores aceites.

Um exemplo de utilização destes especificadores pode ser na configuração do nome das imagens a serem gravadas, como por exemplo, `%v-%Y%m%d%H%M%S-%q`.

Neste caso pode-se ver em baixo o significado de cada especificador:

- %Y = Ano;
- %m = Mês 2 dígitos;
- %d = Data;
- %H = Hora;
- %M = Minutos;
- %S = segundos;
- %T = Formato- HH:MM:SS;
- %v = Evento;
- %q = Numero de *frame*;
- %t = Numero da câmara;
- %D = Pixéis modificados;
- %N = Nível de ruído;
- %i = Comprimento da área em que foi detetado movimento;
- %J = Altura da área em que foi detetado movimento;
- %K = Coordenada x do centro onde foi detetado movimento;
- %L = Coordenada y do centro onde foi detetado o movimento;
- %C = Valor definido pelo *texto_event*.

O servidor *Motion* permite aceder através de uma página *Web* a todas as suas configurações. Para tal na página desenvolvida no âmbito da dissertação de mestrado foi criado uma hiperligação de forma a ser possível ter acesso a esta página, embora esta só deve ser acedida por alguém que tenha alguns conhecimentos técnicos.

O *M-JPEG* é o formato de compressão e transmissão de vídeo utilizado pelo servidor *Motion* em que consiste em uma sequência de imagens *JPEG*. Este formato é amplamente utilizado por câmaras digitais, câmaras por IP e têm suporte nativo pelos *browsers Google Chrome e Mozilla Firefox e Safari*. Este foi o formato escolhido por consumir pouca largura de banda e necessitar de menos recursos de *hardware* sendo assim possível ver o vídeo sem qualquer interrupção devido a problemas de processamento.

Pode-se ver na Figura 33, a página de configuração do servidor *Motion*, onde é possível visualizar e alterar todas as funcionalidades e parametrizações do servidor.

Thread 0

- [daemon](#) = on
 - [process_id_file](#) = /var/run/motion/motion.pid
 - [setup_mode](#) = off
 - [logfile](#) = /home/pi/mmal/motion.log
 - [log_level](#) = 5
 - [log_type](#) = all
 - [videodevice](#) = /dev/video0
 - [v4l2_palette](#) = 17
 - [input](#) = -1
 - [norm](#) = 0
 - [frequency](#) = 0
 - [rotate](#) = 0
 - [width](#) = 640
 - [height](#) = 480
 - [framerate](#) = 2
 - [minimum_frame_time](#) = 0
 - [netcam_url](#) = (not defined)
 - [netcam_userpass](#) = (not defined)
 - [netcam_keeplive](#) = off
 - [netcam_proxy](#) = (not defined)
 - [netcam_tolerant_check](#) = off
 - [filecam_path](#) = (not defined)
 - [mmalcam_name](#) = vc.ril.camera
 - [mmalcam_control_params](#) = (not defined)
 - [mmalcam_use_still](#) = off
 - [mmalcam_raw_capture_file](#) = (not defined)
 - [auto_brightness](#) = off
 - [brightness](#) = 0
 - [contrast](#) = 0
 - [saturation](#) = 0
 - [hue](#) = 0
 - [roundrobin_frames](#) = 1
 - [roundrobin_skin](#) = 1
-

Figura 33 - Página de configuração do servidor *Motion*

3.6.4 Desenvolvimento e apresentação do SVR

No desenvolvimento do protótipo SVR foi necessário a instalação de diversos serviços e pacotes de *software* no Raspberry Pi tal como: servidor *Web*, servidor de *streaming*, servidor de FTP, compilador de PHP e interpretador de *Python*.

Foi desenvolvida uma página *Web* onde é possível fazer todas as configurações do sistema e servidor de *streaming*, ver o vídeo em tempo real, visualizar o arquivo de imagens e vídeos de quando foi detetado movimento pela câmara e fazer o *download* e visualização das mesmas.

É necessário o desenvolvimento diversos scripts para efetuar várias ações como enviar alertas quando houver deteção de movimento, scripts de listagem de ficheiros capturados pela câmara.

Em seguida apresenta-se todos os passos de necessários para a instalação de todos os serviços no *Raspberry Pi*.

Após ter instalado o Sistema Operativo *Raspbian*, distribuição Linux baseada em *Debian*, foi necessário instalar os diversos pacotes de *software*.

O primeiro pacote de *software* a ser instalado foi o servidor de *FTP(VSFTPD)* e o procedimento seguido foi *digitar sudo apt-get upgrade* para obter a informação das últimas versões dos pacotes de software e suas dependências existentes nos repositórios e em seguida, *sudo apt-get install vsftpd*. Terminada a instalação do servidor de *FTP*, foi feita a configuração do mesmo para isso foi editado o ficheiro de configuração através do comando *sudo nano /etc/vsftpd.conf*. Nesse ficheiro foi colocada a seguinte informação:

```
Listen=ON
listen_ipv6=YES
anonymous_enable=off
local_enable=on
write_enable=on
local_root=/home/pi
```

Código 1 – Configuração servidor vsftpd

Para instalar o servidor *Web Apache2* foi introduzido o seguinte comando *sudo apt-get install apache2*.

No servidor *Apache2*, também necessário editar o ficheiro *apache2.conf* normalmente localizado no diretório */etc/apache2/apache2.conf* com a seguinte informação:

```
<Directory />
Options FollowSymLinks
AllowOverride All
Order deny,allow
Allow from all
</Directory>
<Directory /var/www/>
Options Indexes FollowSymLinks
AllowOverride All
Order deny,allow
```

```

        Allow from all
    </Directory>

```

Código 2 – Configuração servidor Apache2

Para instalar o compilador de *PHP5* com suporte para *Mysql* utilizou-se o comando *sudo apt-get install php5 php5-mysql*.

Após instalar estes pacotes de *software* e proceder à sua configuração, procedeu-se para o passo seguinte a instalação do servidor de vídeo. Para instalar o servidor de vídeo *Motion*, escreveu-se os seguintes comandos, *sudo apt-get install motion*, *sudo apt-get install libjpeg62*. Foi necessário alterar o servidor de vídeo para que este funcione com câmaras sem interface USB, como a câmara do *Raspberry Pi* que utiliza o protocolo *MIPI* e interface *CSI-2*, para tal foi necessário proceder ao *download* de um *patch* de configuração em que se utilizou o comando, *wget https://www.dropbox.com/s/0gzxtkxhvwgfofcs/motion-mmal.tar.gz*. Descompactou-se o *patch* utilizando o comando *tar zxvf motion-mmal.tar.gz*. Concluído este processo foi necessário configurar o servidor editando o ficheiro de configuração com o comando *sudo nano motion-mmalcam.conf*.

Os parâmetros mudados no ficheiro de configuração foram os seguintes:

```

daemon on
rotate 0
width 640
height 480
framerate 2
target_dir /var/www/imagens
stream_port 8081
stream_localhost off
Webcontrol_port 8080
Webcontrol_localhost off
on_event_start sudo python /var/www/mail.py

```

Código 3 – Configuração do Servidor Motion

Para ser possível enviar os pacotes de transmissão de vídeo, foi necessário instalar o *modem* de comunicação, o módulo escolhido foi uma *pen* kanguru modelo E1750.

Para utilizar este módulo no *Raspberry Pi* foi necessário instalar o programa *PPPD* para tal foi utilizado o comando *sudo apt-get install pppd*. Instalado este programa for necessário fazer o *download* de um script de configuração(sakis3g⁵³) que permite criar ligações à internet através de um modem 3G. Para o download do script utilizou-se o

⁵³Disponível em: <http://www.sakis3g.com/>

comando `sudo wget "http://www.sakis3g.com/downloads/sakis3g.tar.gz" -O sakis3g.tar.gz`, descompactou-se o ficheiro com o comando `sudo tar -xvzf sakis3g.tar.gz`, e deu-se permissões à pasta do script com o comando `sudo chmod +x sakis3g`. Colocou-se a correr o script com o comando `./sakis3g -- interactive` e este entrou em modo interativo em que é possível configurar o modem 3G.

Para que ligação à rede internet através de o *modem* 3G nunca se desligue procede-se à instalação do *script UMTSkeeper*⁵⁴, em que este mantém sempre a ligação ativa e se esta falhar volta a fazer a remarcação.

Para aceder à câmara de qualquer parte do mundo é necessário configurar um serviço de *DNS*, para não ser necessário conhecer o IP da câmara mas sim seu nome. Para utilizar um serviço *DNS* foi instalado um cliente de *DNS* e o cliente instalado foi o *ddclient*.

Para instalar o cliente de *DNS ddclient*, utilizou-se o comando `sudo apt-get install ddclient`. Em seguida criou-se uma conta no serviço *Web NO-IP*⁵⁵ e procedeu-se à configuração do *ddclient* editando o ficheiro de configuração com o comando `sudo nano /etc/ddclient.conf` e colocando a seguinte informação:

```
use=Web, Web=checkip.dyndns.com/, Web-skip='IP
Address'
protocol=dyndns2
server=dynupdate.no-ip.com
login=your_username
password=your_password
your_domain.com
```

Código 4 - Configuração do cliente dns ddclient

Reiniciou-se o *ddclient* com o comando `sudo service ddclient restart`.

3.6.4.1 Implementação dos sistemas de alerta

Para que o servidor de *stream* envie *emails* de notificação foi criado um script em *Python*, em que este é executado sempre que houver deteção de uma intrusão. Este script vai ler à tabela de notificações na base de dados os utilizadores registados e em seguida envia para esses utilizadores um *email* de alerta, para que estes verifiquem os locais onde se encontra o protótipo de videovigilância (SVR).

Para utilizar o *Python* no acesso ao servidor de *Mysql* foi necessário instalar pacotes correspondentes do *Python* através do comando `sudo apt-get install python-mysqldb`.

⁵⁴Disponível em: <http://mintakaconciencia.net/squares/umtskeeper/>

⁵⁵Disponível em: <http://www.noip.com/>

O script Python contém a seguinte informação:

```
import smtplib
# import the MySQLdb and sys modules
import MySQLdb

# open a database connection
# be sure to change the host IP address, username,
password and database name to match your own
db = MySQLdb.connect(host="localhost",
user="root", passwd="4303660", db="tese")
# prepare a cursor object using cursor() method
cursor = db.cursor ()
# execute the SQL query using execute() method.
cursor.execute ("SELECT * FROM `notificacao` ")
# fetch all of the rows from the query
data = cursor.fetchall ()
# print the rows
for row in data :
    print row[0], row[1],row[2],row[3]
# close the cursor object
cursor.close ()
# close the connection
db.close ()
to = row[3]
gmail_user = 'jaime.r.lopes@gmail.com'
gmail_pwd = 'xxxxx'
smtpserver = smtplib.SMTP("smtp.gmail.com",587)
smtpserver.ehlo()
smtpserver.starttls()
smtpserver.ehlo
smtpserver.login(gmail_user, gmail_pwd)
header = 'To:' + to + '\n' + 'From: ' + gmail_user
+ '\n' + 'Subject:Alerta movimento! \n'
print header
msg = header + "\n Por favor "+ row[1]+"
"+row[2]+", Verifique a camera de videovigilancia.
\n\n"
print msg
smtpserver.sendmail(gmail_user, to, msg)
print 'done!'
smtpserver.close()
```

Código 5 - Script Python de envio de notificações

Este script utiliza duas bibliotecas *smtplib* e *MySQLdb* em que uma têm todos os componentes para ligar a base de dados e assim ter acesso a todos os utilizadores registados para receber alertas. A outra biblioteca (*smtplib*) têm todos os componentes necessários para enviar o *email* com o respetivo alerta. Neste script utilizou-se um *email* do *Gmail* para enviar os respetivos emails. É possível utilizar outro *email*, nomeadamente um email empresarial.

3.6.4.2 Desenvolvimento do Website

Foi desenvolvida uma primeira versão da página *Web* em que foi possível testar todas as funcionalidades e opções. Nesta primeira versão foi utilizado unicamente HTML, CSS e PHP.

Para proteger o acesso à página *Web* foi criado um formulário de acesso em que é necessário inserir o utilizador e a palavra-chave de acesso. Estes dados podem ser alterados depois de o utilizador fazer o acesso. O formulário de acesso faz uso de variáveis de sessão, foi necessário dar permissões ao diretório onde são armazenadas através do comando `sudo chmod -R 777 /var/lib/php5/`.

Pode-se ver na Figura 34 a página do formulário de autenticação onde é feito a verificação das credenciais de acesso para aceder a todo o conteúdo da página *Web*.



Figura 34 - Janela de autenticação de utilizador

Após a autenticação do utilizador a página *Web* é redirecionada para a página principal que é possível visualizar na Figura 35.



Figura 35 - Página principal com acesso ao vídeo stream

Na página principal existe um menu do lado esquerdo em que é possível aceder a todas as opções como ver o vídeo, alterar o acesso à página, listar as imagens e os vídeos, apagar imagens e vídeos, configurar o correio eletrónico das notificações e também aceder às páginas de configuração do servidor.

Na Figura 36, é possível ver a janela da página onde é possível mudar as credenciais de acesso à página *Web*.

The image shows a web interface for ISEP (Instituto Superior de Engenharia do Porto). At the top, there is a dark red header with the ISEP logo and name. Below the header, there is a white rectangular area containing a login form. The form has two input fields: 'Username' and 'Password'. To the right of the 'Password' field is a button labeled 'Change'. The entire form is set against a dark red background.

Figura 36 - Janela de alteração de credenciais de acesso

Na Figura 37, pode-se ver a listagem de todas as imagens e vídeos que foram capturados pela câmara aquando a deteção de uma intrusão.

Descrição

































Filename		
	01-20150322165538.avi 	01-20150322171336.avi 
01-20150322171933.avi 	01-20150322172301.avi 	01-20150322172434.avi 
01-20150322173538.avi 	01-20150322173852.avi 	01-20150322182834-01.jpg 
01-20150322182836-00.jpg 	01-20150322182836-01.jpg 	01-20150322182837-00.jpg 
01-20150322195634-00.jpg 	01-20150322195634.avi 	01-20150322195635-00.jpg 
01-20150322195636-00.jpg 	01-20150322195636-01.jpg 	01-20150322195637-00.jpg 
01-20150322195638-00.jpg 	01-20150322195638-01.jpg 	01-20150322195639-00.jpg 
01-20150322195640-00.jpg 	01-20150322195640-01.jpg 	01-20150322195641-00.jpg 
01-20150322195642-00.jpg 	01-20150322195642-01.jpg 	01-20150322195643-00.jpg 
01-20150322195644-00.jpg 	01-20150322195644-01.jpg 	01-20150322195645-00.jpg 
01-20150322195646-00.jpg 	01-20150322195646-01.jpg 	01-20150322195647-00.jpg 

Figura 37 - Janela de listagem de vídeos e imagens

Na tabela da Figura 37 pode-se ver todas as imagens e vídeos armazenados pelo servidor *Motion*. O nome dos ficheiros armazenados seguem a estrutura data e hora de captura do movimento de forma a ser fácil para o utilizador identificar as imagens que deseja consultar e analisar. Todos os ficheiros terminam com a sua extensão para ser possível ao utilizador identificar se é uma imagem (extensão JPG) ou um vídeo (extensão avi). Nesta opção de listar os ficheiros em tabela também é possível apagar imagens e vídeos carregando na cruz vermelha à frente do nome do ficheiro.

Na Figura 38, pode-se ver o formulário para inserir o correio eletrónico da pessoa que irá receber as notificações.

The screenshot shows a web form with a dark red header. The header contains the ISEP logo (a stylized 'i' and 'sep' with a vertical line) and the text 'Instituto Superior de Engenharia do Porto'. Below the header, there is a form with three input fields: 'Nome' (containing 'jaime'), 'Apelido' (containing 'lopes1'), and 'Email' (containing 'streamtuga@gmail.com'). A 'Change' button is located below the email field.

Figura 38 - Janela de inserção de correio eletrónico para notificações

No final de terem sido verificadas todas as funcionalidades da página *Web*, concluiu-se que era necessária melhorar graficamente a página *Web*, como também torna-la responsiva, de forma a ter um bom funcionamento gráfico em qualquer dispositivo de que se aceda.

Procedeu-se então ao desenvolvimento de uma segunda versão da página *Web* em que para além do *HTML*, *CSS*, *PHP*, optou-se por utilizar uma *framework* chamada *Bootstrap* em que está utiliza *HTML*, *CSS*, *JS* e é vocacionada para o desenvolvimento de *Websites* responsivos. Nesta nova versão da página *Web* todas as funcionalidades se mantiveram, mudando unicamente o aspeto gráfico da mesma.

Nas imagens seguintes pode-se ver o aspeto das diferentes janelas que constituem a página *Web*. Em que na Figura 39 pode-se ver a janela de autenticação do utilizador para dar acesso às diferentes opções que estão disponíveis ao utilizador.

The screenshot shows a web browser window with the address bar displaying '192.168.1.5/index.php'. The page has a dark blue header with the ISEP logo and a 'Home' link. The main content area is light gray and features a login form. The form has a lock icon at the top, followed by two input fields: 'Username' and 'Password'. Below these fields is a blue button labeled 'Entrar'.

Figura 39 - Versão 2 da janela de autenticação de utilizador

A Figura 40 é a página principal da página *Web* em que se pode ver as diferentes opções disponíveis para o utilizador bem como ver o do protótipo (SVR) em tempo real.



Figura 40 - Versão 2 da página principal com acesso ao vídeo *streaming*

Na Figura 41 é possível visualizar a página onde é possível alterar as credenciais de acesso à página *Web* do SVR.

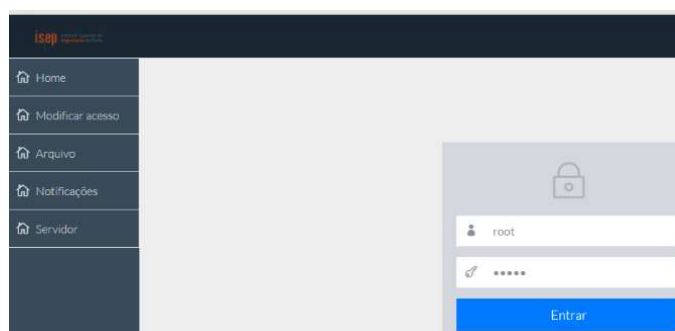


Figura 41 - Versão 2 da página de alterar as credenciais de acesso

Na Figura 42, é possível ver a opção de arquivo onde se pode ver todas as imagens e vídeos capturados pela câmara na deteção de uma intrusão.

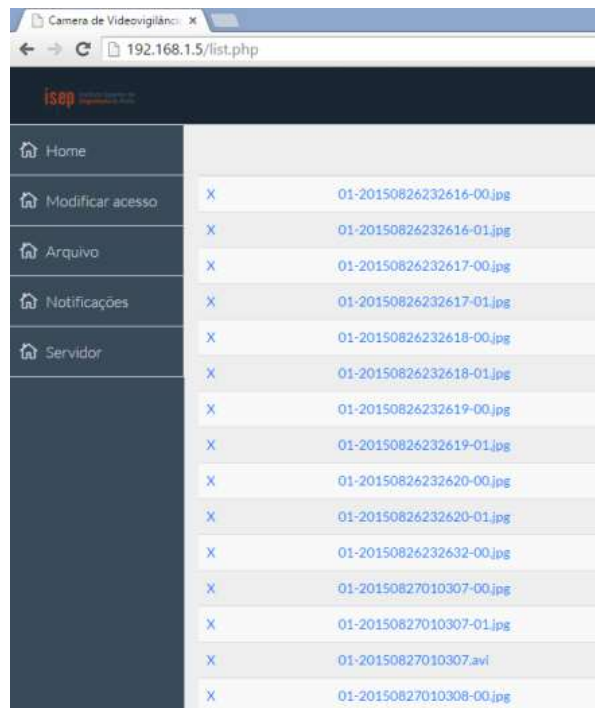


Figura 42 - Versão 2 da página de listar o arquivo de imagens e vídeos

Na Figura 43, pode-se ver a opção de alterar os dados para o envio de notificações através de correio eletrónico.

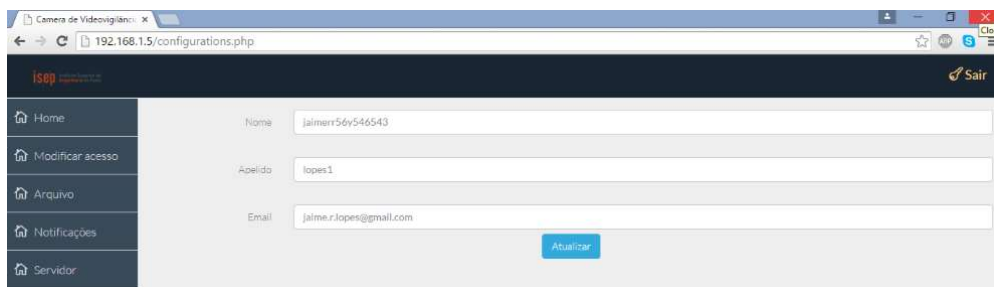


Figura 43 - Versão 2 da página de altera correio eletrónico das notificações

Por último temos a Figura 44, em que se pode ver a página de configuração do servidor em que é possível alterar todos os parâmetros de configuração do mesmo, como tamanho da imagem, rotação, frequência de captura, entre outras.



Figura 44 - Página de configurações do servidor

3.6.4.3 Base de dados

Para o protótipo de videovigilância (SVR) foi criado uma base de dados com duas tabelas, uma utilizada na autenticação do utilizador na página *Web* e outra para armazenar os dados referentes aos utilizadores que vão receber os alertas gerados pela câmara no momento da deteção de movimento.



Figura 45 - Tabela de utilizadores

Na imagem da Figura 45 pode-se ver a tabela de armazenamento de utilizadores que têm como nome (Login), em que o nome do utilizador é armazenado na variável *username* e a palavra-chave na variável *password*. Estes dados são utilizados na autenticação da página do protótipo do sistema de videovigilância (SVR).

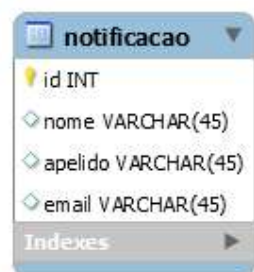


Figura 46 - Tabela de armazenamento de os dados para o envio de notificações

Na Figura 46 pode-se ver a tabela com o nome (notificação), em que neste são armazenados os dados da pessoa que receberá as notificações provenientes do protótipo SVR a informar que houve uma deteção de intrusão. Esta tabela é constituída por quatro variáveis, id, nome, apelido e *email*. Em que no id é gravado o índice da tabela, no nome e apelido será armazenado primeiro e ultimo nome da pessoa que irá receber o *email* e por ultimo será gravado o email para onde serão enviadas as notificações.

Para auxiliar na criação da base de dados foi instalado o *phpMyAdmin*, através do comando `sudo apt-get install phpmyadmin`. No processo de instalação foi necessário configurar *phpMyadmin* conforme as seguintes figuras:

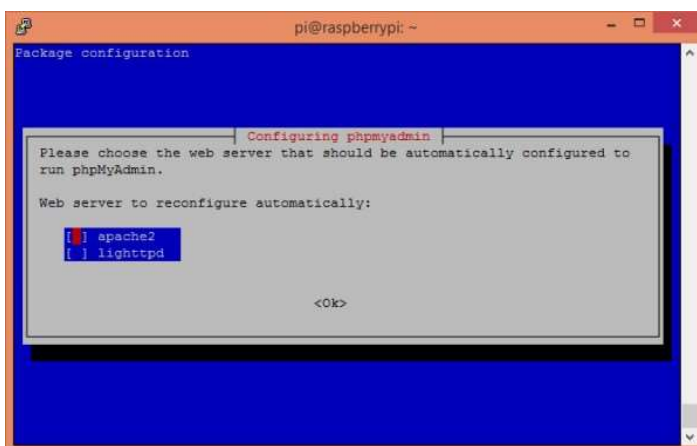


Figura 47 - Seleção do servidor de Web

Nesta Figura 47 pode-se ver um menu de configuração na fase de instalação do *phpmyadmin*, em que se define o tipo de servidor *Web* que será utilizado em que no caso do protótipo SVR será o servidor *Web Apache*.

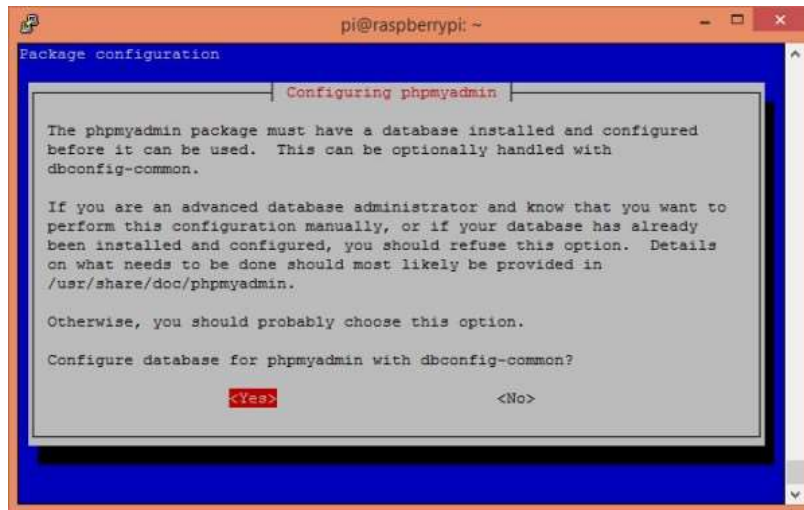


Figura 48 - Utilização do *dbconfig-common*

Na Figura 48 pode-se ver a continuação do processo de configuração do *phpmyadmin*, em que se escolheu a opção de utilizar o *dbconfig-common*.

O *dbconfig-commom* consiste na implementação automática de todas as configurações e instalação de pacotes necessários ao funcionamento do *Phpmyadmin* e da base de dados.

Também foi pedido para inserir as palavras-chaves de acesso ao servidor de *Mysql* e também para definir a palavra-chave e utilizador para o *PhpMyadmin*.

No final da instalação foi necessário editar o ficheiro de configuração do apache através do comando `sudo nano /etc/apache2/apache2.conf`, em que se acrescentou no final a seguinte linha `Include /etc/phpmyadmin/apache.conf`.

3.6.4.4 Hardware do sistema de videovigilância

Neste ponto pode-se ver a descrição de todo o *hardware* que compõe a câmara de videovigilância. Esta é essencialmente constituída poder uma unidade de central de processamento que no nosso caso é o *Raspberry Pi*, conversor DC/DC, controlador de carga, painéis solares, *modem* de comunicação de dados e bateria.

3.6.4.5 Conversor DC/DC STEP-UP

No protótipo desenvolvido foi necessário a utilização de um conversor de tensão DC/DC, com topologia *STEP-UP*, devido à natureza da bateria utilizada em que a sua tensão nominal é inferior à do *Raspberry Pi*.

Na Figura 49, pode-se ver o circuito impresso do conversor elevador de tensão. Este conversor converte a tensão da bateria 3,7V em 5V, que é a tensão nominal de funcionamento do *Raspberry Pi* e do *modem* de comunicação de dados.

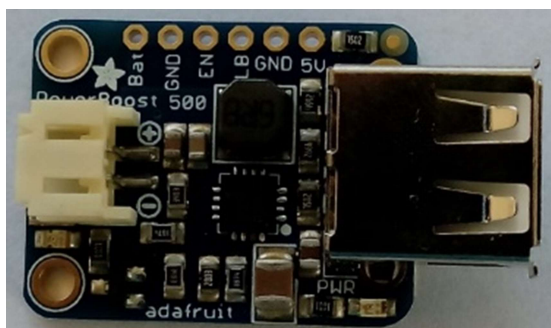


Figura 49 - Conversor DC-DC STEP-UP

O coração deste conversor é o IC TPS61090 *boost* converter da *Texas Instruments*. Este integrado têm as seguintes características: proteção interna de 2A, conversão síncrona, capacidade de funcionar com frequência de comutação de 700kHz, eficiência acima dos 90% e capacidade de supervisionar a tensão da bateria. Este conversor consegue disponibilizar pelo menos 1A, a partir de uma bateria de 3.7V LiPoly/Lítio.

3.6.4.6 O Controlador de carga

O controlador de carga é responsável pela gestão de energia e carga da bateria. Este circuito está ligado à bateria, painéis solares e também ao conversor de tensão.

Este é responsável por extrair o máximo de energia do painel fotovoltaico e fornecer esta aos restantes circuitos do protótipo, carregar a bateria utilizada sempre que esta se encontre sem carga.

Na Figura 50, pode-se ver a placa de circuito impresso do controlador de carga utilizado no protótipo SVR.

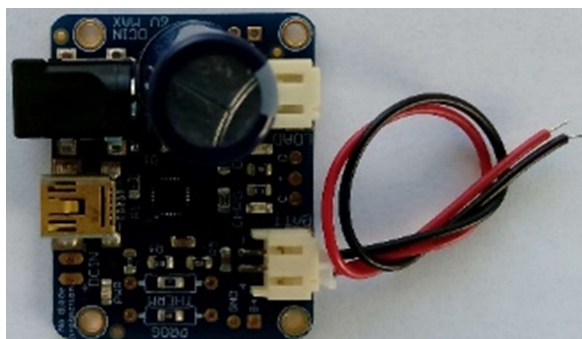


Figura 50 - Controlador de carga

Este controlador de carga está preparado para baterias de 3,7/4,2V de íões de lítio ou de lítio polimérico e é alimentado através de uma fonte de alimentação com uma tensão de 5/6VDC, USB ou com painel solar de 6V de tensão nominal. Este controlador de carga dispõe de três leds de sinalização que informam quando a alimentação do mesmo está nos parâmetros admissíveis, informação que está a carregar a bateria e bateria carregada. Este têm uma corrente máxima de carga de 500mA que pode ser ajustada entre 50 mA e 1A e para além disso este têm a capacidade de dragar o máximo de corrente do painel fotovoltaico mesmo não sendo um MMPT.

O controlador de carga é responsável por fazer o carregamento da bateria respeitando o seu ciclo de carga de forma a não a danificar e aumentar o seu tempo de vida.

3.6.4.7 Bateria de lítio Polimérico

A bateria que alimenta o circuito da câmara é de Lítio Polimérico (LiPo), que são baterias com dimensões mais reduzidas, mais robustez e com capacidade de ter diferentes formas. Estas baterias têm uma tensão nominal de 3,7V e têm diferentes capacidades de armazenamento.

A capacidade da bateria necessário para que o sistema funcione durante o dia e a noite é de aproximadamente 10Ah no Verão e de aproximadamente 15Ah no Inverno, isto conforme o número de horas de luz disponíveis durante o dia.

Na Figura 51, pode-se ver a imagem da bateria utilizada no protótipo de videovigilância (SVR).

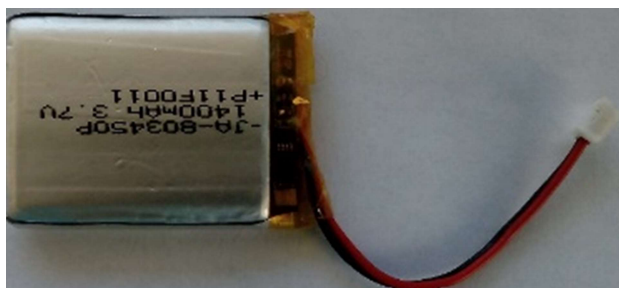


Figura 51 - Bateria LiPo

3.6.4.8 Raspberry Pi e a Picam

O cérebro de todo o sistema é a placa de desenvolvimento *Raspberry Pi*. É nesta placa de circuito impresso que estão instalados todos os pacotes de *software* (servidor de vídeo, servidor *Web*, servidor *mysql*, interpretador de *Python*, *PHP*) que tornam realidade a câmara de videovigilância (SVR).

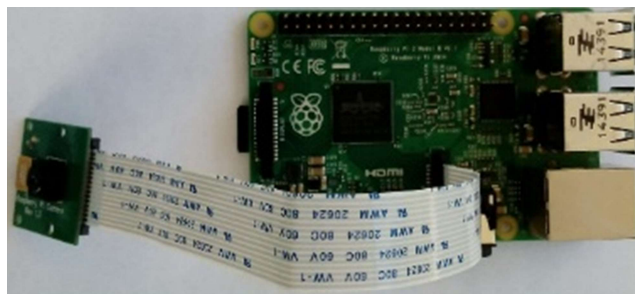


Figura 52 - Raspberry Pi com a Picam

3.6.4.9 Assemblagem de todos os componentes do sistema

Os componentes foram todos ligados entre si para executarem diferentes funções e todos juntos formam o protótipo de videovigilância (SVR) conforme se pode ver na Figura 53.

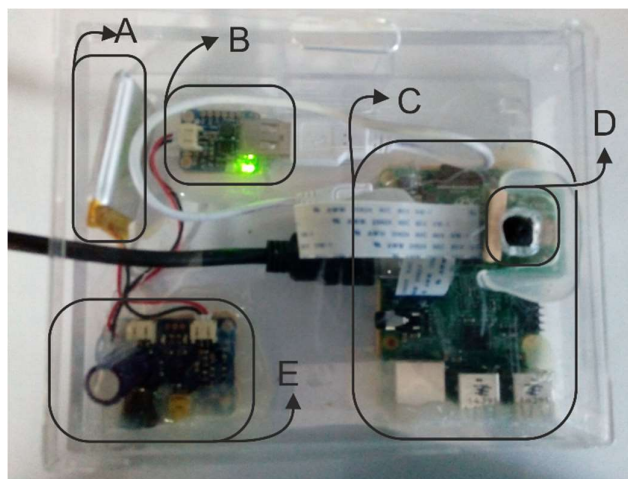


Figura 53 - Todos os componentes da câmara *assembledos*

Legenda:

- a) Bateria de lítium;
- b) Conversor DC/DC;
- c) *Raspberry Pi*;
- d) Câmera de vídeo;
- e) Controlador de carga.

3.6.4.10 Os painéis fotovoltaicos

Para o projeto foram escolhidos três painéis solares policristalinos, com uma potência de 3,5W cada um, tensão nominal de 6V. AS dimensões por painel são de 135mm x 165mm com um peso de 90g.

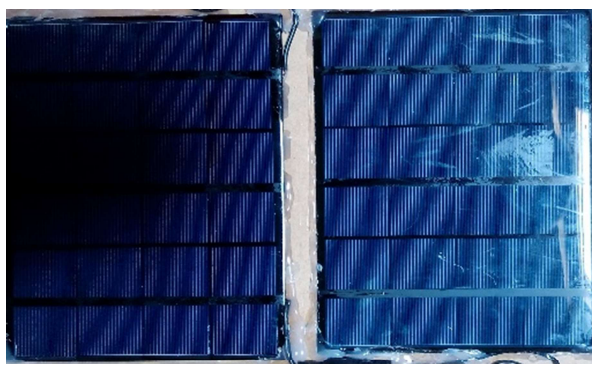


Figura 54 - Painéis fotovoltaicos

Os três painéis solares foram ligados em paralelo de forma a manter a tensão nominal aos seus terminais mas aumentar a corrente total que pode ser disponibilizada ao circuito que vão alimentar. Como os painéis foram ligados em paralelo foi necessário

colocar um díodo de proteção entre eles para o caso de haver correntes inversas ou curto-circuitos.

A potência total fornecida pelos painéis solares é de 10.5W, isto porque a câmara de videovigilância em funcionamento e com o *modem* de comunicação de dados ligado têm um consumo de aproximadamente 5W.

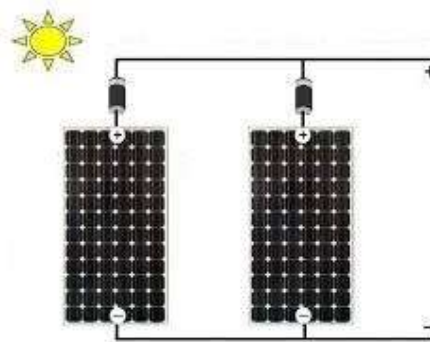


Figura 55 - Esquema de ligação painéis fotovoltaicos⁵⁶

Para que o sistema funcione em pleno durante o dia e noite a potência total necessária de painéis solares é superior a 22W para que seja possível fornecer 1A de consumo instantâneo e outros 3,3A para carregar a bateria necessária para o funcionamento nas horas que não existe luz solar.

Durante o inverno Portugal têm uma média de 4 a 6 horas de luz e durante o verão 10 a 12 horas⁵⁷, isto implica que é necessário obter energia suficiente durante as horas de luz para que o sistema funcione durante a noite. O sistema necessita de uma corrente nominal de 1A para funcionar logo é necessário uma bateria de aproximadamente 20Ah para que o sistema opere durante o inverno que é o pior caso.

$$\text{Horas de funcionamento} = \frac{\text{Capacidade da bateria}}{\text{Corrente nominal do sistema}} = \frac{20\text{Ah}}{1\text{A}} = 20\text{h}$$

$$\text{Corrente necessária de carga} = \frac{\text{Capacidade da bateria}}{\text{Horas de luz solar}} = \frac{20\text{Ah}}{6\text{h}} = 3, (3)\text{A}$$

⁵⁶ Disponível em:

<https://www.google.pt/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0CAcQjRxqFQoTCOHfk-HD08cCFcwq2wodZ5QHgz&url=http%3A%2F%2Fwww.mpptsolar.com%2Fpt%2Fpaineis-solares-em-paralelo.html&ei=WGTkVeG5FMzV7AbnqJ7wDA&psig=AFQjCNGR5IMqZpTWi02g3cb0at3okUmgoQ&ust=1441117404158773>

⁵⁷ Disponível em: https://pt.wikipedia.org/wiki/Clima_de_Portugal

$$\begin{aligned} \text{Potência dos painéis fotovoltaicos} &= \text{Tensão nominal} \times \text{Corrente total} \\ &= 5 \times (1 + 3,3) = 21,5W \cong 22W \end{aligned}$$

Com uma capacidade de 20Ah o sistema consegue funcionar durante as 18h em que não existe luz solar. Com uma potência solar instalada de 22W é possível manter o sistema em funcionamento e efetuar o carregamento da bateria para que o sistema funcione durante os períodos em que não existe luz solar.

Pretende-se no futuro fazer um estudo experimental de forma a confrontar a análise teórica de forma a entender se é possível ter o sistema SVR em funcionamento 24 horas por dia sem que seja necessário alterar a sua forma de funcionamento.

3.6.4.11 A estrutura exterior do sistema de videovigilância SVR

Pretendemos que o SVR seja um dispositivo camuflado para que este não seja notado nos locais em que é colocado para vigiar. Este deve ser capaz de se misturar com a fauna, flora e relevos do local em que está inserido como se de um camaleão se tratasse. Desta forma é difícil a perceção e localização por parte dos intrusos não correndo o risco de serem danificadas por estes.

Na Figura 56 pode-se ver o aspeto final do SVR com a forma de uma rocha em que é possível colocar este em locais rochosos ou uma vegetação idêntica.



Figura 56 - Estrutura camuflada do sistema de videovigilância SVR

3.6.4.12 O local de colocação do protótipo

A câmara de videovigilância deve ser colocada no local conforme a finalidade a que se destina, os locais podem ser divididos conforme a função que irá desempenhar a câmara que são os seguintes:

- Vigilância de intrusos;
- Vigilância de bens (físicos, animais);

A câmara de videovigilância deve ser colocada num local estratégico de forma a estar em linha de vista com o tipo de bem (mercadorias, gado, animais, frutos) a proteger. Como tal deve ser colocada num local não exposto ao olhar de intrusos e que esteja camuflada pela envolvente.

Na Figura 57, pode-se ver um exemplo de colocação do SVR em um caminho que dá acesso a diferentes edifícios. Este está colocado de forma estratégica de forma a ser possível captar qualquer tentativa de intrusão a um dos edifícios e enviar notificação ao utilizador para que este verifique o local ou previna as autoridades competentes se realmente se verificar a intrusão.

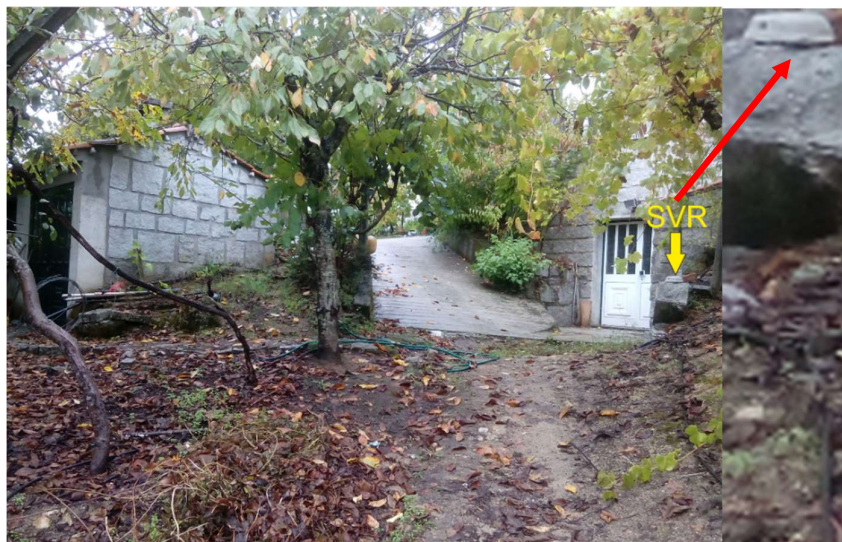


Figura 57 - O SVR a vigiar um local de acesso

4 Testes e validação do sistema SVR

*"A ciência só pode determinar o que é, não o que deve ser,
e fora de seu domínio permanece a necessidade
de juízos de valor de todos os tipos."*

Albert Einstein

Neste capítulo apresentam-se todos os testes realizados durante o desenvolvimento do sistema SVR como os testes efetuados no fim do seu desenvolvimento como validação e avaliação do protótipo, em que são avaliados diversificados parâmetros como camuflagem, facilidade de montagem, autonomia de bateria, recuperação do sistema numa falha total de energia, envio de notificação na deteção de movimento, espaço ocupado em disco. Por último apresenta-se a análise geral do protótipo em que são demonstrados os resultados da avaliação e validação efetuada.

4.1 Testes realizados no desenvolvimento

Durante o processo de desenvolvimento, e principalmente, na fase final do projeto foram realizados diversos testes ao sistema. Estes tiveram como objetivo verificar se as funcionalidades estavam a ser desenvolvidas de acordo com os objetivos que o sistema tinha de responder.

Na Figura 58, pode-se ver a câmara a fazer *streaming* de vídeo para a página Web, em que a ligação à internet foi feita através do *modem* 3G da *Kanguru*.

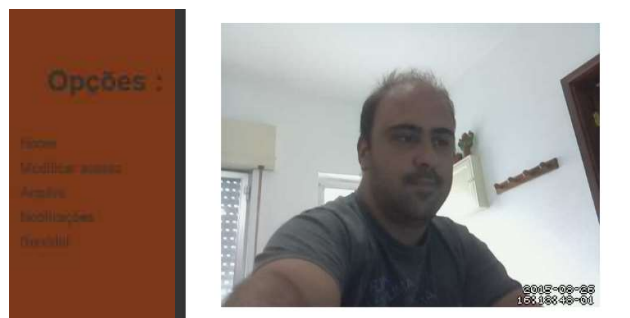


Figura 58 - Página com *streaming* de vídeo

O teste de visualização do vídeo foi feita à distância em que a câmara se encontrava na cidade do Porto e o utilizador que se encontrava a visualizar o vídeo encontrava-se na cidade de Barcelos. Não houve qualquer dificuldade na visualização e utilização dos recursos da página *Web*.

Após ter sido detetado movimento a câmara enviou um alerta para o correio eletrónico definido, pode-se ver esse *email* na Figura 59. Nesta mensagem vêm o nome da pessoa que deveria receber a notificação e uma mensagem a pedir ao utilizador para verificar a câmara.

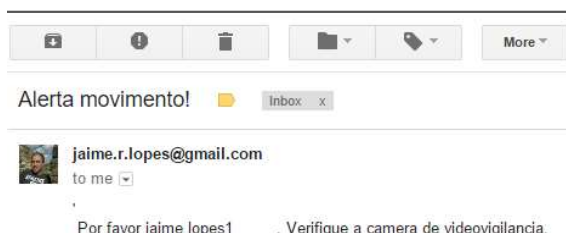


Figura 59 - *Email* de notificação

Carregando no menu na opção de servidor, teremos acesso à página de configuração de todas as opções do servidor *Motion*, aqui é possível alterar todas as configurações conforme se pode ver na Figura 60.



Figura 60 - Página de configuração do *Servidor Motion*

Procedeu-se também aos testes da versão 2 da página de internet e tudo correu como planeado, visto que todas as funcionalidades já estavam implementadas e testadas, tendo unicamente mudado toda a parte gráfica da página *Web*.

Na Figura 61, pode-se ver a imagem do vídeo na nova página *Web*.

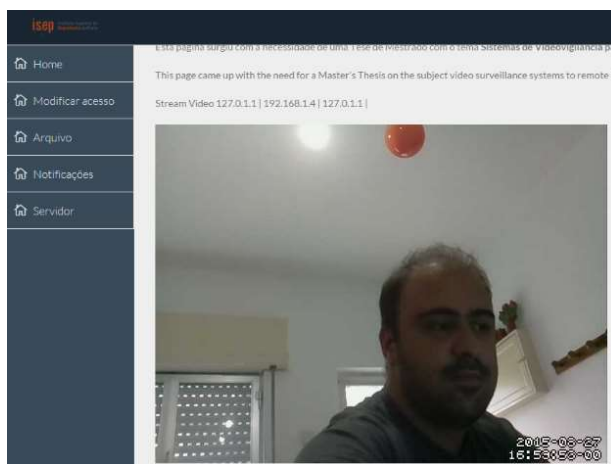


Figura 61 - *Streaming* de vídeo na versão 2 da página *Web*

Na Figura 62 e na Figura 63, pode-se ver a câmara de videovigilância instalada em um local a ser vigiado e a ser alimentada por um painel fotovoltaico.



Figura 62 - Câmera de videovigilância e painel fotovoltaico

Na figura abaixo pode-se ver o local que se pretende vigiar que é um barracão que serve de arrumos a alfaías agrícolas em que também é possível ver o sistema de videovigilância SVR já colocado no local e operacional, nestes testes de campo em que o desenvolvimento não se encontrava finalizado não houve o cuidado de camuflar o SVR para que este não fosse detetado.



Figura 63 - Local a ser vigiado pela câmara de videovigilância

Na Figura 64, pode-se ver a imagem do vídeo capturado pela câmara de videovigilância no local rural que se pretendia vigiar. Este vídeo foi capturado pela câmara a ser alimentada pelo painel fotovoltaico e os dados pelo *modem* de comunicação de dados (*Pen kanguru*).



Figura 64 - Imagem do vídeo capturado pela câmara de vigilância

4.2 Testes do protótipo SVR

Para avaliar o protótipo ao sistema de videovigilância SVR, foram realizados testes indoor e *outdoor* de forma a analisar o seu funcionamento e verificar o grau de satisfação de cumprimento de todos os objetivos bem como detetar eventuais problemas e proceder a resolução dos mesmos.

Para proceder aos testes o sistema foi ligado e procedeu-se à simulação de intrusões de forma a verificar a sua resposta e também validar todas as opções que são oferecidas pelo mesmo.

4.2.1 Testes indoor ao sistema SVR

Foram realizados diversos testes *indoor* na fase de desenvolvimento e validação do protótipo.

Na fase de validação o protótipo do sistema de videovigilância (SVR) foi instalado e colocado em funcionamento em uma sala de aula do Instituto Superior de Engenharia do Porto com recurso à energia elétrica.

Como é possível observar na imagem abaixo, sempre que o estado original do espaço (porta fechada) sofria alguma alteração, mesmo que ligeira o sistema era acionado dando origem à captura de imagens e de vídeos.



Figura 65 - Sensibilidade à intrusão em espaços interiores

Na imagem seguinte, apresenta-se um conjunto de imagens com intuito de ilustrar cada uma das intrusões ocorridas. Nas imagens de cima pode ver-se o orientador deste estudo que foi convidado a passar em momentos distintos à frente do protótipo. Por baixo estão uma série de ícones representativos de algumas das inúmeras ocorrências de entrada. As primeiras imagens serviram apenas para verificar se o SVR estava operacional e a cumprir os objetivos de captura. Após essa fase os alunos começaram a entrar e cada nova ocorrência o sistema reagiu favoravelmente.

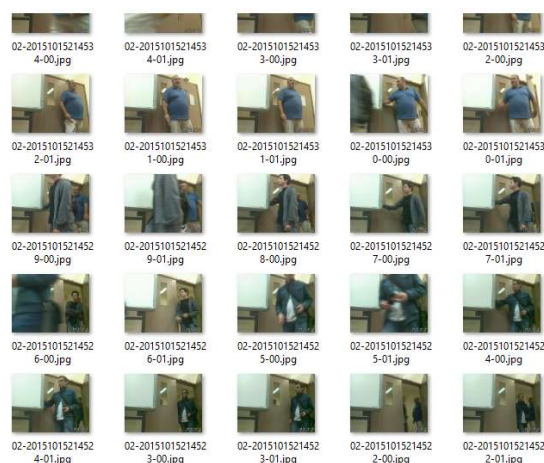


Figura 66 - Ocorrências de intrusão durante testes num espaço interior

No final, todas as imagens capturadas pelo SVR durante a ocorrência de intrusões geram automaticamente um vídeo onde é possível visualizar as entradas.

A imagem abaixo ilustra esse mesmo vídeo com a duração de 3:56 minutos, uma resolução de 640x480, tamanho de 6,76MB e um *bitrate* de 500Kbps.



Figura 67 - Vídeo gerado pelo SVR com todas as ocorrências de intrusão

Os videos gerados, são arquivados com um nome baseado nos dados da ocorrencia como data e hora sendo que, no caso numa determinada data existirem várias ocorrencias é acrescentado o numero inteiro que é repetido quantas vez quanto os videos gerados.A imagem abaixo mostra um excerto de um desses videos cujo o nome é 02-20151015214133 que significa que no dia (15 de Outubro de 2015-20151015) foi o segundo video gerado pelo sistema (02-) sendo que neste caso o video foi criado pelas 21 horas, 41 minutos e 33 segundos.

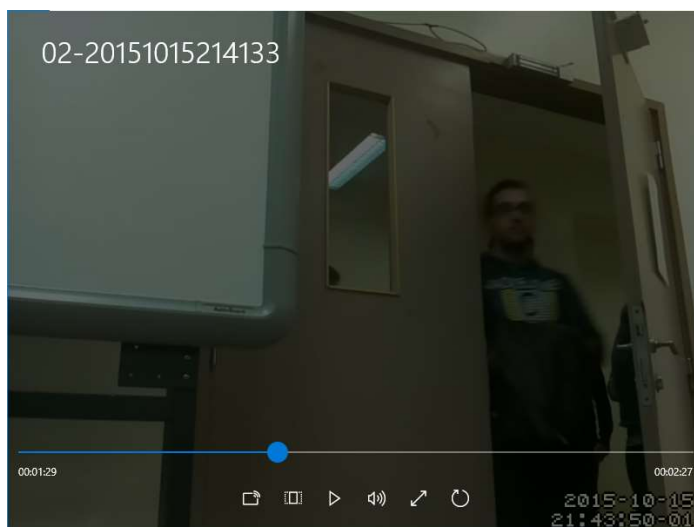


Figura 68 - Vídeo gerado pelo SVR

Ao vídeo, como se ilustra na figura seguinte são adicionadas informações que permitem correlacionar as ocorrências espaço-temporais sendo acrescentada a data e a hora em que está a ocorrer o que se vê.

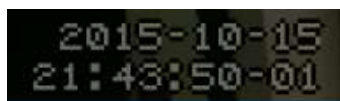


Figura 69 - Dados adicionados ao vídeo (data e hora)

Durante a visualização é possível termos outras informações como o tempo onde decorre um determinado fenómeno sendo ainda possível ver através de uma linha temporal com ícone azul em forma de círculo onde nos encontremos no vídeo.

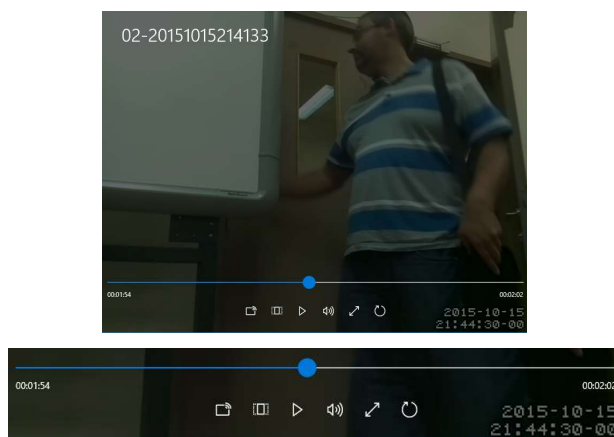


Figura 70 - Mecanismo de navegação no *player* do vídeo

Deste modo o utilizador pode navegar pelo vídeo deslocando-se para um ponto do mesmo onde existe uma ocorrência que lhe interesse analisar em detalhe.

Ao longo do tempo são gerados inúmeros vídeos provenientes do mais variado tipo de ocorrências de intrusão. A qualquer momento, o utilizador pode a partir de sua casa aceder á página *Web* do SVR e efetuar o *download* do vídeo que pretender.

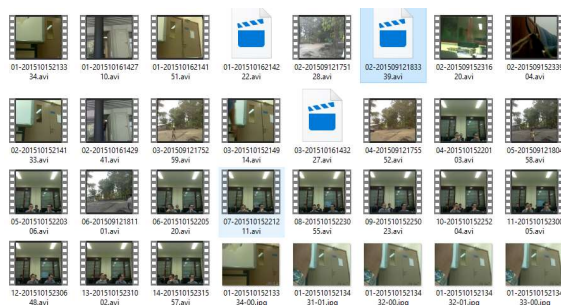


Figura 71 – Lista de vídeos na máquina do utilizador após *download*

Durante os testes efetuados no interior foram tiradas inúmeras imagens como a que se apresenta abaixo onde, a cada nova entrada na sala era tirada uma foto conforme se pode na imagem seguinte (Figura 72).



Figura 72 - Testes indoor do sistema SVR em uma sala de aula

A imagem seguinte pretende ilustrar um conjunto de testes que permitissem analisar a durabilidade de captura de imagens enquanto existisse uma intrusão para o efeito colocamos o SVR desenvolvido num átrio da empresa onde trabalha o autor e como se pode ver na figura seguinte, foram capturadas fotos continuamente de 1 em 1 segundo até que o intruso deixasse de estar dentro da área de captura.



Figura 73 – Teste à área de intrusão

Na figura anterior, percebe-se que começam a ser capturadas imagens a partir do momento que o intruso entra na área de intrusão terminando esta captura (que foi para já preparada ser realizada de segundo a segundo) apenas quando o intruso sai de cena. Á semelhança dos testes realizados anteriormente estes testes foi gerado um vídeo que pode ser visualizado a qualquer momento pelo utilizador bastando para isso ao utilizador aceder à página *Web* do protótipo SVR.

4.2.2 Testes outdoor do protótipo SVR

O sistema de videovigilância SVR esteve em testes em diversos locais no exterior, onde se pretendeu testar todas as suas funcionalidades bem como fazer a sua avaliação. Os locais foram escolhidos como sendo potenciais locais para receber no futuro um sistema SVR ou idêntico. Um dos locais é uma entrada de acesso a uma casa de habitação conforme se pode ver Figura 76 e outro é um cruzamento que dá acesso a uma casa e a um barracão de arrumos de alfaías agrícolas conforme se pode ver na Figura 74.



Figura 74 - Cruzamento com sistema SVR instalado

O sistema de videovigilância SVR esteve em funcionamento durante algum tempo nesta localização (Figura 74), onde foi possível detetar várias intrusões nomeadamente uma delas a de um veículo juntamente com um animal conforme se pode ver na imagem da Figura 75.



Figura 75 – Imagem capturada pelo SVR em teste

Durante este teste foi possível identificar diferentes intrusos que passaram por este local inclusive identificar um veículo confirmando a capacidade do sistema de videovigilância (SVR) funcionar como dispositivo de vigilância para este tipo de locais.



Figura 76 - Local de acesso com o sistema SVR instalado

Em esta Figura 76, encontra-se o sistema de videovigilância (SVR) instalado e em funcionamento, em um local de acesso em que foi possível detetar diversos intrusos em que na Figura 77 pode-se ver uma dessas intrusões.



Figura 77 – Imagem capturada pelo SVR em teste em um local de acesso

Apesar de estar num local oculto de modo, tornar-se indetetável ao intruso, com estes testes foi possível perceber alguns aspetos importantes. A qualidade da imagem mesmo com alguma distância neste caso uns 10 metros permite com a luz diurna identificar claramente o intruso. Da experiencia ilustrada pela figura anterior foi ainda possível perceber que o local escolhido para colocar a câmara não foi o melhor pelo fato de ter folhagens à frente que se moviam com o vento e por esse aspeto ativavam constantemente o sistema. Permitiu uma reflexão sobre a colocação do protótipo que

deve ser feita apenas em áreas onde a alteração do fundo seja mínima ou bastante reduzida.

4.3 Avaliação do sistema de videovigilância SVR

De forma a validar o protótipo SVR, foram criados alguns pontos de validação que se poderão categorizar nas seguintes categorias:

- Camuflagem do protótipo;
- Camuflagem do protótipo;
- Facilidade de montagem
- Autonomia da bateria;
- Recuperação do sistema numa falha total de energia elétrica;
- Envio de notificação na deteção de movimento;
- Espaço ocupado em disco pelos vídeos/imagens capturadas.

4.3.1 Camuflagem do protótipo SVR

O objetivo desta dissertação é desenvolver um dispositivo de videovigilância para locais remotos para deteção de intrusões que em grande parte se manifestam em delitos, crimes e atos de vandalismo. Como tal é essencial que o sistema de videovigilância seja o mais furtivo possível de forma a passar despercebido para o indivíduo que pretende cometer esses atos menos idóneos. Como se pretende instalar o sistema de videovigilância SVR normalmente em propriedades privadas que sejam isoladas e que não tem qualquer tipo de vigilância é possível que o mesmo esteja escondido de forma a não ser visível, pois o enquadramento legal deste tipo de sistemas não abrange a instalação em locais privados exceto se os sistemas pretendem capturar imagens e vídeos de um local de acesso público, em que aí é necessário ter uma licença de utilização bem como avisos de como o local se encontra sobre vigilância.

Como o sistema de videovigilância SVR será instalado maioritariamente em locais rurais, estes normalmente têm uma paisagem característica com árvores, e diversos tipos de rochas (pedras), como tal pretende-se que o sistema se misture o máximo com a paisagem envolvente, então procedeu-se ao desenvolvimento de uma estrutura para albergar todos os componentes do sistema que se assemelha a uma rocha conforme se pode ver na Figura 78.



Figura 78 - Estrutura camuflada do sistema de videovigilância SVR

Pode-se ver que a estrutura desenvolvida para este protótipo se assemelha a uma pequena rocha que facilmente se coloca em paisagens onde exista relevos e rochas em que assim este facilmente se torna invisível para qualquer intruso.

Pretende-se que no futuro existam diversas estruturas para albergar o sistema com diferentes formas, cores, tamanhos, de forma a ser possível colocar o sistema nos mais diversos espaços de forma a não ser identificado e assim desempenhar a sua função de detetar possíveis infrações nos espaços que estão a ser vigiados sem que os indivíduos se apercebam da sua presença.

4.3.2 Facilidade de montagem

O sistema de videovigilância foi pensado para que seja possível ser colocado em funcionamento por qualquer pessoa independente da sua idade, estatura ou conhecimentos técnicos.

Para colocar o sistema de videovigilância SVR em funcionamento basta determinar qual o melhor local de forma a este estar em linha de visto com o que se pretende vigiar e que este não esteja visível ou que então que se misture com a paisagem envolvente. E em seguida instalar em um local próximo mas que seja soalheiro a fonte de energia solar o

painel solar fotovoltaico de forma a este trabalhar à sua potência nominal para que este forneça a energia necessária para o funcionamento do sistema de videovigilância SVR. Após a instalação destes dois componentes, o sistema de videovigilância e a sua fonte de energia basta conectar os dois e o sistema entra automaticamente em funcionamento. Ao fim de efetuar a instalação do sistema no local, será só necessário introduzir em um *browser* de navegação na *Web* o endereço do dispositivo para que seja possível visualizar o vídeo em tempo real que está a ser adquirido pelo sistema de videovigilância bem como proceder a todas as opções do sistema de videovigilância SVR. Pode-se dizer que é um sistema extremamente fácil e intuitivo de colar em funcionamento sendo um dispositivo bastante *user friendly* em termos de montagem do ponto de vista do utilizador.

4.3.3 Autonomia de bateria

A autonomia de uma bateria é uma das características mais importantes de qualquer sistema eletrónico que seja alimentado através destas. O nosso sistema utiliza uma bateria de forma a armazenar energia para que seja possível o sistema funcionar nos períodos de ausência de luz solar e durante o período noturno. A bateria e o controlador de carga utilizados no nosso protótipo estão subdimensionados para as necessidades do sistema e funcionamento atual isto traduz-se que na ausência de sol ou períodos noturnos o sistema funciona por um curto período de tempo de aproximadamente uma hora e trinta minutos. Esta situação pode ser facilmente ultrapassada através da aquisição de uma bateria com maior capacidade e com um controlador de carga adequado para a potência envolvida, isto traduz-se em um custo mais elevado para o sistema. Uma forma de maximizar a eficiência do sistema de forma a este consumir menos energia elétrica e assim aumentar a duração da bateria e diminuir a capacidade de armazenamento necessária, seria criar um algoritmo e programar o sistema de forma a este só transmitir através do *modem* de comunicação móveis só quando o utilizador desejar ou então quando é detetado movimento em que o sistema liga o modem e envia a notificação. Isto porque neste momento o sistema de videovigilância está permanentemente ligado á internet a transmitir o *stream* de vídeo o que faz com que o sistema tenha uma necessidade permanente de uma corrente elétrica 1000 mA o que significa uma potência nominal de 5W.

O sistema de videovigilância SVR com o algoritmo implementado em que o *modem* de comunicação móvel só liga quando é necessário faria com que este passasse a consumir

uma corrente de aproximadamente 200mA o que se traduziria numa potência nominal de 1W. Isto em termos práticos traduz-se que com uma simples bateria de 2000mAh que é uma bateria inferior à utilizada por qualquer *smartphone* atual daria para aproximadamente 10 horas de funcionamento o que seria suficiente para o sistema de videovigilância SVR estivesse em funcionamento durante todo o período noturno até ao nascer do sol de forma a voltar a carregar essa mesma bateria e assim repetir o ciclo. O controlador de carga de bateria faz com que esta só seja carregada quando está abaixo de um determinado nível de capacidade o que se traduz numa maior duração desta pois assim serão cumpridos os ciclos de carga e descarga desta de forma a aumentar o máximo a sua substituição.

O nosso protótipo SVR neste momento utiliza para o seu funcionamento uma bateria de lítio polimérico com uma capacidade de 2000mA, em que este tipo de bateria têm a característica de terem dimensões mais pequenas e uma grande capacidade e um elevado número de ciclos de carga e descarga.

As baterias tendem a se danificar ou a diminuir o seu tempo devido quando estão sujeitas a temperaturas elevadas, como o sistema SVR vai ser instalado em locais rurais em que normalmente as temperaturas nesses locais atingem valores consideráveis e este pode-se encontrar a céu aberto será considerado a necessidade de no futuro a estrutura do sistema tenha um isolamento térmico e que tenha ventilação se for possível. Assim o sistema SVR não sentirá as alterações das amplitudes térmicas sentidas no exterior e através da ventilação será possível libertar o calor gerado no interior por todos os componentes eletrónicos e assim aumentar a durabilidade de todos os componentes principalmente da sua bateria.

4.3.4 Recuperação do sistema numa falha total de energia elétrica

Conforme se pode ver no ponto 4.3.3, a autonomia e o sistema de alimentação são sistemas críticos e que estão sujeitos a grande *stress*. Existe uma remota possibilidade de o sistema ficar sem energia elétrica devido a problemas de bateria ou ausência de luz solar que não se traduz na carga da respetiva bateria. O sistema na ausência de energia elétrica devido a uma falha do sistema de alimentação traduz-se em o sistema AVR desligar. Se a falha tiver sido causada pela ausência de luz solar quando esta voltar a estar disponível o sistema volta a entrar em funcionamento normal de operação. Como o

sistema não dispõe de qualquer tipo de sensor de medição da capacidade da bateria que esteja diretamente ligado ao sistema de controlo implica que na ausência de energia elétrica o sistema irá desligar sem fazer o correto encerramento do sistema operativo podendo corromper o sistema de ficheiros e danificar os ficheiros necessários ao seu arranque. Pretende-se que no futuro o sistema de gestão de energia do SVR que é constituído pelo controlador de carga, bateria forneça o estado da bateria ao sistema de controlo de forma que se implemente um algoritmo que sempre que a bateria está com a capacidade demasiado baixa este faz o encerramento do sistema operativo e desliga todo o sistema até que a bateria se encontre com capacidade para voltar a colocar em operação todo o sistema. Assim evita-se que o sistema seja desligado sem fazer o devido encerramento do sistema operativo permitindo assim que este não seja danificado e assim eliminar qualquer risco de o sistema SVR fique inoperacional. O não encerramento do sistema operativo implica que seu sistema de ficheiros possa ficar danificado, sendo necessário fazer a recuperação dos ficheiros corrompidos ou a reinstalação do sistema operativo para que o sistema SVR volte a ficar operacional.

4.3.5 Envio de notificação na deteção de movimento

A principal função do sistema SVR é detetar quando existe alguma intrusão e notificar o utilizador do sistema. Sendo esta uma função bastante crítica da parte funcional o sistema foi colocado no exterior em teste de forma a mesurar a quantidade de notificações que ele falhou ou seja houve uma intrusão e este não detetou e também o número de notificações falsas ou seja não houve qualquer intrusão mas por algum motivo o sistema deu um falso alarme, na tabela abaixo pode-se ver uma pequena tabela com os resultados obtidos.

Horas de funcionamento	Tipo teste	Intrusões efetuadas	Intrusões reais detetadas	Falsas intrusões detetadas
2	Outdoor	6	5	3
1	Indoor	3	3	--
3	Indoor	3	3	--

Tabela 4 Tabela de análise das deteções de movimento.

Ao analisar a tabela pode-se verificar que o sistema teve melhor desempenho em funcionamento no interior de um edifício do que enquanto em funcionamento no

exterior. Isto porque num edifício o ambiente é controlado não existe variáveis como o vento que no exterior este provoca que a vegetação se agite e se esta estiver e linha de vista com o sistema de videovigilância SVR é possível conforme se pode ver na tabela existir falsos alarmes. Para minimizar falsos alarmes é necessário determinados cuidados na escolha do local a vigiar, ter em conta o tipo de vegetação e a distância desta ao SVR, pode também ser necessário ir à página de configuração do servidor e ajustar os valores de *threshold*, que consiste em alterar o número de pixéis diferentes entre *frames* para que este detete como uma deteção de movimento. Também é possível verificar que nos testes no exterior houve uma deteção que o sistema não detetou.

Nos testes realizados no interior o sistema foi 100% assertivo, isto porque as condições são controlados, não existindo os problemas que podem existir no exterior como vento, chuva, animais.

4.3.6 Espaço ocupado em disco pelos vídeos/imagens capturadas

O sistema de videovigilância SVR sempre que deteta movimento captura as imagens e cria um vídeo que fica gravado na sua memória, isto traduz-se em espaço ocupado na sua memória física. Sempre que o utilizador recebe a notificação que foi detetado movimento este pode aceder à página *Web* do SVR e visualiza as imagens e vídeos capturados na presença de movimento. A duração do vídeo e quantidade de imagens capturadas é diretamente proporcional à duração do movimento o que implica na possibilidade de o sistema preencher por totalmente a sua memória é possível verificar a quantidade de memória ocupada na página *Web* e assim o utilizador ter o cuidado de eliminar as imagens e vídeos mais antigos de forma a libertar o espaço físico disponível para futuras capturas. A página *Web* dispõe da funcionalidade de o utilizador ver os vídeos e imagens capturadas e fazer o seu armazenamento no seu computador e apagar as imagens e vídeos no dispositivo.

Cada imagem gravada em memória pelo dispositivo ocupa 61.5KB, o vídeo depende da duração do movimento. As imagens são gravadas em formato JPEG e o vídeo em formato em *.avi.

No futuro pretende-se que o sistema seja capaz de gerir a quantidade de informação armazenada e este funcionar de formar a ter uma armazenamento circular em que sempre que é preenchida na totalidade a sua memória física este começa a apagar as

imagens e vídeos mais antigos de forma a libertar espaço em disco, esta solução pode trazer outro problema que é o utilizador não fazer os respetivos *backups*, para que não se perca qualquer informação. Pretendesse que o sistema faça backup automático da informação num servidor em um serviço como a *Dropbox*⁵⁸, *Onedrive*⁵⁹ da Microsoft ou o *Drive*⁶⁰ da Google.

4.4 Análise geral ao protótipo SVR

Para proceder à avaliação do protótipo do sistema de videovigilância (SVR), este foi instalado e colocado em funcionamento em dois locais distintos. Um dos locais foi no centro de Nanotecnologia Materiais técnicos, Funcionais e Inteligentes (Centi⁶¹) e uma sala de aula do Instituto Superior de Engenharia do Porto (ISEP). Os funcionários do Centi e os alunos do ISEP responderam a um inquérito para avaliar o SVR, na totalidade 21 pessoas responderam a este inquérito.

Em seguida pode-se ver os resultados desses mesmos inquéritos começando pela caracterização da população alvo.



Gráfico 1 - Distribuição da população alvo quanto ao sexo

Em este Gráfico 1, pode-se observar que a população masculina está em larga maioria, com 71% da população inquirida. A população feminina representa 29%, estando representados em minoria.

⁵⁸Disponível em: www.dropbox.com

⁵⁹ Disponível em: <https://onedrive.live.com/about/pt-pt/>

⁶⁰ Disponível em: <https://drive.google.com/drive/>

⁶¹Disponível em: www.centi.pt

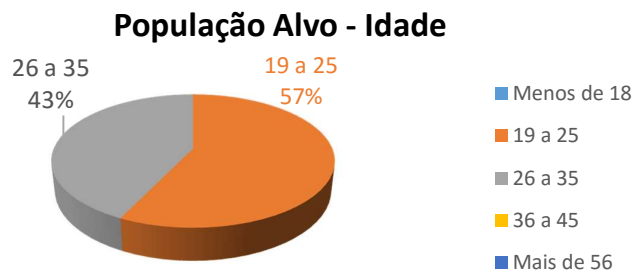


Gráfico 2 - Distribuição da população alvo quanto à idade

Em relação à idade dos inquiridos o Gráfico 2 apresenta a seguinte distribuição: Entre os dezanove e os vinte e cinco anos, 57%; Com idades entre os vinte e seis e os trinta e cinco anos 43%. Permitindo concluir que a população inquirida incidu maioritariamente sobre uma população alvo, jovem.



Gráfico 3 - Distribuição da população alvo quanto às habilitações literárias

Quanto às habilitações literárias dos inquiridos, estes distribuem-se: Licenciatura, 67%; Mestrado, 28%; Décimo segundo ano 5%. Observando-se que 95% dos inquiridos têm formação superior.

A totalidade das pessoas inquiridas respondeu que os sistemas de videovigilância são uteis. O que indica que os sistemas de videovigilância são aceites pela sociedade e que são reconhecidos como sendo uma ferramenta útil na prevenção e dissuasão de diferentes crimes e assim tornam a sociedade mais segura.

Análise á população alvo -Contato com sistemas de videovigilância

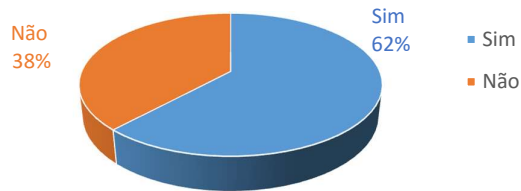


Gráfico 4 - Percentagem de inquiridos que já tiveram contacto com sistemas de videovigilância

Neste Gráfico 4 pode-se verificar que 62% já tiveram contato com sistemas de videovigilância.

Este é um dado de grande importante para a análise da população alvo que está a proceder à avaliação de um protótipo de um sistema de videovigilância para locais remotos. Sendo assim possível realizar uma avaliação mais concisa fazendo um contraste com os sistemas de videovigilância com quais os indivíduos da população inquirida já tiveram contato.

Análise á população alvo -Serão uteis os sistemas de videovigilância para locais remotos

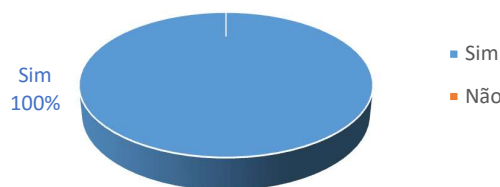


Gráfico 5 - Percentagem de inquiridos que acham os sistemas de videovigilância para locais remotos uteis

Através da análise deste gráfico pode-se verificar que toda a população inquirida acha os sistemas de videovigilância para locais remotos sem energia elétrica uma solução útil.

Análise á população alvo -Adquiria um sistema de videovigilancia para locais remotos

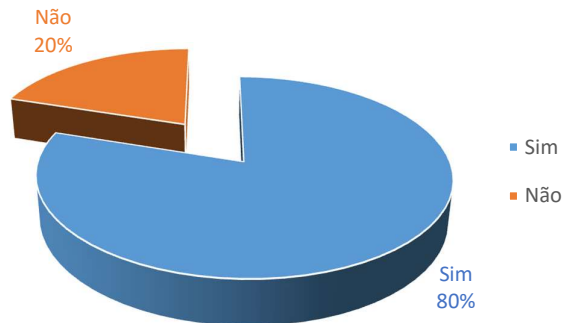


Gráfico 6 - Percentagem de inquiridos possivelmente adquiria um sistema de videovigilância para locais remotos

Neste gráfico verifica-se que 20% não adquiria um sistema de videovigilância para locais remotos em contraste com os 80% que certamente ponderava em comprar um sistema. Esta análise reflete a existência de uma necessidade, procura para este tipo de sistemas de videovigilância.

Análise á população alvo -A camuflagem é importante

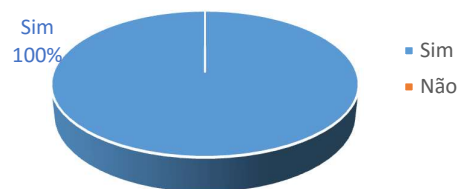


Gráfico 7 - Percentagem de inquiridos que acha importante a camuflagem no sistema de videovigilância

A totalidade dos inquiridos acha importante a camuflagem em um sistema de videovigilância.

Um sistema de videovigilância camuflado têm menor risco de ser descoberto e assim é possível reduzir o risco de este ser destruído.

Avaliação da camuflagem do sistema de videovigilância (SVR)

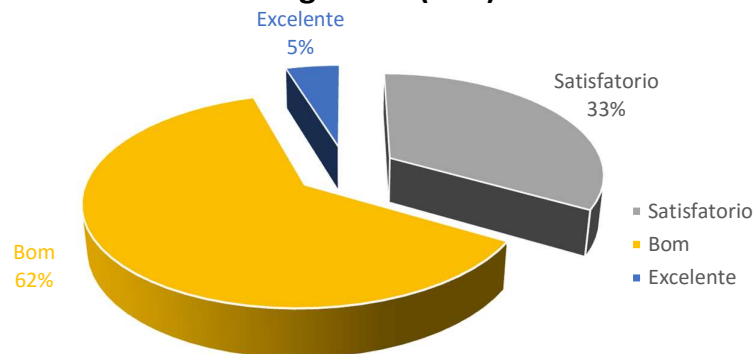


Gráfico 8 – Distribuição da população alvo em relação à camuflagem do protótipo SVR.

Neste gráfico a população inquirida distribui-se da seguinte em relação à sua opinião sobre a camuflagem do protótipo SVR: 62% dos inquiridos têm a opinião que o protótipo SVR têm um bom camuflamento; 33% dizem que o camuflamento do SVR é satisfatório; 5% dos inquiridos acha o camuflamento excelente.

O protótipo SVR pela avaliação da população alvo têm um bom camuflamento o que se pode traduzir em uma difícil deteção por parte dos intrusos, logo é possível fazer uma melhor vigilância pois o risco de este ser descoberto e destruído é menor.

A montagem do sistema de videovigilância(SVR) é simples

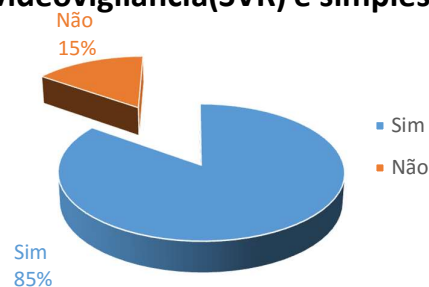


Gráfico 9 – Distribuição da população alvo em relação à montagem do protótipo SVR

Em relação à montagem do protótipo SVR a população inquirida distribui-se da seguinte forma: 85% disseram que sim a montagem é simples; 15% disseram que a montagem não é simples.

Estes dados dizem-nos que a população inquirida têm a opinião que a montagem do sistema SVR é bastante simples o que é um ponto positivo neste tipo de sistemas.

Usabilidade do sistema de videovigilância(SVR)

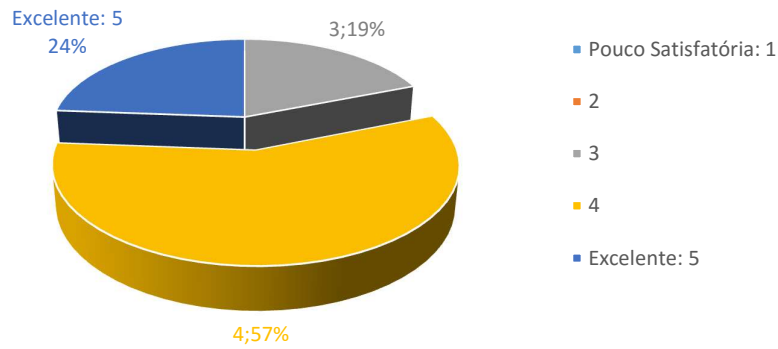


Gráfico 10 – Distribuição da população em relação à usabilidade do protótipo SVR

Para classificar o sistema de videovigilância (SVR) em relação à sua usabilidade foi necessário criar uma escala de 1 a 5 em que o 1 significa uma usabilidade pouco satisfatória e o 5 uma usabilidade excelente. Em que por análise do Gráfico 10 pode-se verificar que 24% dos inquiridos avalia a usabilidade do sistema SVR como excelente classificando com 5 e 57% classifica este com 4 o que está próxima de excelente, 19% dos inquiridos acham simplesmente satisfatória classificando com 3.

Com estes dados pode-se afirmar que o sistema SVR têm uma usabilidade excelente o que se traduz em uma fácil utilização da mesmo.

Inovação do sistem de videovigilância (SVR)

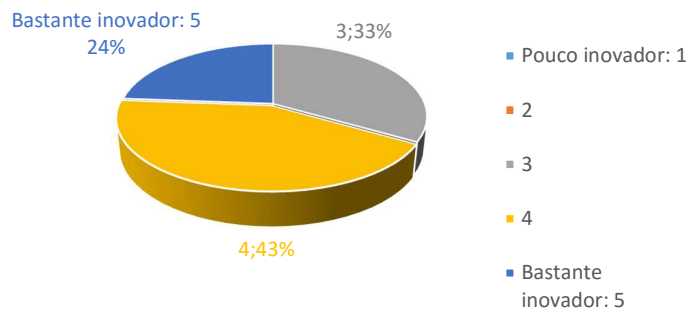


Gráfico 11 – Distribuição da população em relação à inovação do protótipo SVR

Para avaliação da inovação do protótipo de videovigilância SVR foi criado uma escala de 1 a 5 sendo o número 1 indicativo de pouco inovador e o 5 de bastante inovador. Analisando o Gráfico 11 o pode-se verificar que 24% da população classificou com 5 o SVR e 43% classificou com 4 indicado que este é bastante inovador os restantes 33% classificou o SVR com 3 o que significa que para este a inovação não é um ponto de destaque do SVR.

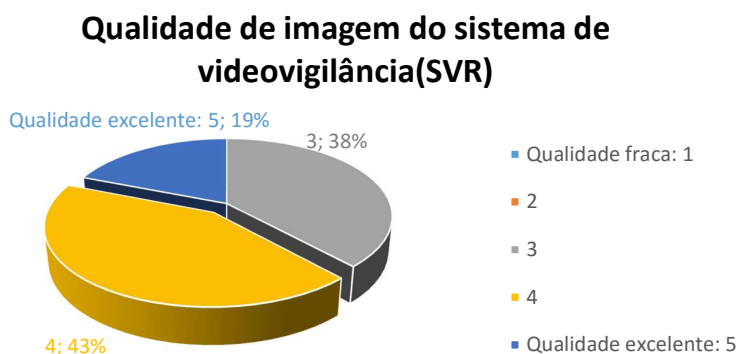


Gráfico 12 - Distribuição da população em relação à qualidade de imagem do protótipo SVR

Para avaliar a qualidade de imagem do SVR foi criada uma escala de 1 a 5 em que 1 é equivalente a uma qualidade de imagem fraca e o 5 uma qualidade de imagem excelente. Analisando o Gráfico 12 pode-se verificar que 19% classificou com 5 e 43% classificou com 4 a qualidade de imagem do SVR o que é equivalente a dizer que a qualidade de imagem do sistema SVR é excelente, 38% dos inquiridos classificou com 3 a qualidade de imagem o que indica que esta satisfaz embora não seja excelente.

Deteção de movimento pelo sistema de videovigilância(SVR)

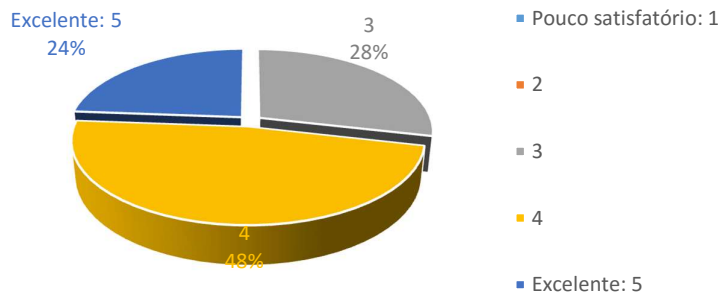


Gráfico 13 – Distribuição da população em relação à detecção de movimento pelo protótipo SVR

Para analisar a capacidade do sistema de videovigilância (SVR) em detetar intrusões foi criado uma escala de de 1 a 5 em que o 1 significa pouco satisfatório e o 5 excelente.

Traduzindo o Gráfico 13, pode-se verificar que a opinião dos inquiridos em relação á detecção de intrusão pelo sistema de videovigilância (SVR), é a seguinte: 25% dos inquiridos classificam com 5 e 48% com 4 em que isto se traduz que o SVR têm uma excelente capacidade de detetar intrusões e 28% dos inquiridos dizem que o SVR satisfaz em relação à detecção de intrusões.

5 Conclusões e trabalho futuro

“O homem é tão bom quanto seu desenvolvimento tecnológico o permite ser.”

George Orwell

O presente capítulo é reservado às conclusões e análise crítica do estudo efetuado nesta dissertação em que foi detetado um problema na vigilância de locais remotos predominantemente agrícolas a qual se pretendeu desenvolver uma possível solução. Serão abordadas as limitações da solução proposta e desenvolvida e apresenta-se os possíveis desenvolvimentos futuros para tornar o protótipo em um produto comercial.

5.1 Conclusões e análise crítica

Nos últimos anos houve uma massificação dos sistemas de videovigilância que passaram a ser utilizados nos mais diversos locais, devido ao clima de insegurança e medo que as pessoas sentem em consequência do crescimento de alguns crimes como assaltos, vandalismo e situações de violência.

Com esta dissertação de mestrado pretendeu-se responder a um problema que foi identificado que é a ausência de vigilância em locais remotos essencialmente rurais e agrícolas onde é inexistente infraestruturas que permitam a adoção de meios tecnológicos de videovigilância.

Em estes locais têm havido um aumento de furtos nomeadamente de alfaías agrícolas, gado, culturas e colheitas agrícolas consequência de não existir vigilância por ausência de infraestruturas necessárias para a videovigilância e por não ser economicamente viável a presença de vigilantes e também devido ao risco a que estes profissionais estariam sujeitos em termos de integridade física e psicológica por os locais ser isolados e fora das áreas de habitação.

Para dar resposta a este problema foi desenvolvido um protótipo de um sistema de videovigilância (SVR) que é autónomo de energia elétrica recorrendo ao uso de painéis fotovoltaicos e a baterias, em que quando a existência de rede móvel é possível realizar o *streaming* de vídeo desses locais bem como efetuar a deteção de intrusos e enviar

alertas para os utilizadores desse sistema. Se não houver cobertura da rede móvel o sistema é capaz de detetar intrusos e gravar as imagens e vídeos dessas ocorrências para posteriormente visualizar.

O protótipo permite que o utilizador tenha a capacidade de visualizar o vídeo em tempo real em qualquer parte do mundo através de um *browser* de internet.

A página *Web* do protótipo SVR foi construída de forma responsiva para que possa ser acedida por qualquer dispositivo, PC, *tablet*, *smartphone*, sendo só necessário colocar o endereço da mesma, através desta página *Web* é possível ver o vídeo em tempo real, consultar o arquivo das imagens capturadas na deteção de intrusão bem como apagar as mesmas, alterar o *email* do utilizador que receberá as notificações como também alterar as diversas opções do servidor.

A instalação do protótipo SVR é extremamente simples sendo necessário unicamente colocar a o protótipo no local a ser vigiado e os seus painéis solares estarem exposto aos raios solares.

O protótipo foi colocado em funcionamento no terreno com a alimentação a ser realizada através dos painéis solares fotovoltaicos em que este, esteve a operar e foi possível testar a sua capacidade de capturar diversas intrusões nomeadamente veículos, pessoas e animais e receber posteriormente a notificação da intrusão.

Um dos detalhes do protótipo que foi dado um grande ênfase foi na sua capacidade de camuflagem em que foi realizada uma estrutura camuflada com aspeto de uma rocha de forma a ser possível colocar este em diversos locais sem que seja notada a sua presença pelos intrusos e assim ser possível a sua identificação ou mesmo a captura no ato de cometer o delito.

Este mesmo protótipo foi colocado em funcionamento numa sala de aula do Instituto Superior de Engenharia do Porto de forma a ser possível validá-lo através de um inquérito colocado aos alunos presentes.

Através da análise das respostas dos inquiridos aos inquéritos podemos concluir que os sistemas de videovigilância são essenciais para a sociedade e que existe uma necessidade de este tipo de sistemas em locais remotos onde não existe infraestruturas como energia elétrica.

Na avaliação e validação do protótipo de videovigilância (SVR), por parte da população alvo podemos dizer que este tem uma boa camuflagem é fácil a sua montagem e colocação em funcionamento e a sua qualidade de imagem é excelente. Em relação à sua

capacidade de detecção de intrusões a população alvo classificou como excelente e boa e classificou o mesmo como sendo um protótipo bastante inovador.

Podemos concluir que o protótipo desenvolvido é uma solução para a vigilância em locais remotos, em que este certamente será um mecanismo de dissuasão e redução de crimes, furtos em estes locais, bem como poderá ser uma ferramenta de ajuda no combate ao flagelo dos incêndios nomeadamente porque com este será possível detetar os incêndios na sua fase de ignição e assim evitar que este se expanda minimizando os danos provocados, reduzindo assim os prejuízos económicos, ambientais, sociais.

Em termos desta dissertação podemos concluir que os objetivos foram cumpridos, foi identificado um problema de grande relevo que é a ausência de vigilância em locais rurais, remotos e sem infraestruturas para a videovigilância em que foi colocado e desenvolvido um protótipo como possível solução deste problema. Em que este protótipo cumpriu todos os requisitos propostos como sendo fulcrais para dar uma solução ao nosso problema.

Em termos pessoais esta dissertação permitiu-me conhecer melhor o problema existente na área da vigilância principalmente nas áreas rurais e remotas. Permitiu-me obter novas competências e conhecimentos em diversas áreas como na área de desenvolvimento *Web* em que houve a necessidade de trabalhar com base de dados (*MYSQL*), *framework Bootstrap*, *PHP*, *HTML*, *CSS*, *Python*. Na área da eletrotecnia fazer a integração de diversos componentes e tecnologias como painel fotovoltaico, controlador de carga, conversor DC/DC.

Assim de uma maneira global faz-se um balanço positivo do desenvolvimento e do protótipo obtido em que é possível com o continuar deste desenvolvimento tornar este protótipo em um produto.

5.2 Trabalho Futuro

O protótipo de sistema de videovigilância (SVR) desenvolvido como solução ao problema identificado nesta dissertação para que esta se torne num produto pronto a entrar no mercado é necessário um desenvolvimento na área de *design* de produto, de forma a criar uma câmara com um aspeto o mais camuflado possível para que esta possa ser colocada em locais remotos diversificados com diferentes faunas e floras que necessitem de vigilância sem que se identifique a presença da mesma.

Também será necessário preparar a câmara de videovigilância para que esta funcione em ambientes de pouca luz ou inexistência da mesma. Como tal será necessário integrar uma luz de infravermelhos que liga no período noturno ou de pouca luz, esta luz não é perceptível para o ser humano.

Em termos de funcionalidades o próximo passo seria a implementação da funcionalidade de tirar fotografias sempre que o utilizador assim o deseja-se e a transferência automática de imagens e vídeos para um servidor externo sempre que seja detetado uma intrusão de forma que se a câmara sofrer danos ou for alterada indevidamente haver um *backup* de dados num servidor externo.

O Sistema SVR necessita de diversas otimizações na área da gestão da energia elétrica, nomeadamente em só ligar o *modem* de comunicação de dados a quando a deteção de intrusão de forma a este não estar permanentemente ligado e assim reduzir a necessidade de uma bateria de grande capacidade para que este funcione vinte e quatro horas por dia em constante vigilância. Embora esta solução teria de ser analisada pois ao desligar o *modem* de comunicação de dados deixa de ser possível para o utilizador interagir com o sistema à distância.

É intenção do autor, iniciar uma nova etapa relacionada com a escrita científica no sentido de apresentar o presente estudo à sociedade e a todos aqueles que de algum modo têm interesse no presente tema.

A participação em conferências *workshops* ou palestras na área fará parte do trabalho futuro onde, e por acreditarmos que este trabalho têm um valor social relevante e que pode contribuir para a diminuição de criminalidade como por exemplo roubos ou deteção de incêndios em locais remotos faz parte dos horizontes do autor.

5.3 Considerações finais

Acreditamos que o protótipo aqui desenvolvido e apresentado pode contribuir para a resolução do problema identificado.

As avaliações técnicas realizadas ao longo de inúmeros testes dentro e fora de espaços físicos e sobretudo as realizadas em espaços rurais, onde para além de não existir energia elétrica não tinham cobertura de qualquer rede *Wifi* e onde o acesso à internet terá de ser feito apenas por *pens* de banda larga mostrou que o protótipo ficou totalmente operacional capturando e guardando qualquer tipo de intrusão e durante o tempo que ela ocorria.

Foi evidenciado que todos que tomaram contacto com ele o consideraram extremamente útil e com enorme potencial para proporcionar a videovigilância em locais remotos.

Temos consciência que se trata apenas de um protótipo e que muito terá de ser feito para chegar a uma solução final e sobretudo até ser possível banalizar sua utilização neste tipo de espaços.

Foi nossa preocupação que o protótipo para além das funcionalidades que aqui ficaram demonstradas tivessem duas outras características essenciais:

- Um preço reduzido – O que veio a comprovar-se pelo fato de ser suportado por um *Raspberry Pi*, cartão de memória, *pen* de banda larga, bateria e painel fotovoltaico cujo custo total ronda os 100 euros. É possível que o custo venha aumentar se melhorarmos alguns destes aspetos como a duração da bateria, capacidade do cartão de memória e a potência do painel fotovoltaico;
- Capacidade de camuflagem – Pelo fato de se tratarem de componentes reduzidos a sua inserção dentro de outros objetos (inclusivamente objetos que fazem parte dos espaços que se pretendem vigiar como por exemplo um troco ou pedra simulada feita de barro) torna o sistema bastante mais eficaz pelo fato de não ser detetável.

Consideramos que com a aplicação e uso de um protótipo desta natureza e a sua replicação pelas florestas e espaços rurais deste nosso país poderíamos contribuir para a diminuição de incêndios e de roubos contribuindo assim para uma sociedade mais segura e com menos criminalidade.

Para além disso, percebemos que este protótipo pode ser usada em outros ambientes e fins com intuito de contribuir para uma sociedade mais segura e com menos criminalidade.

Referências

- [Ao.at al,2009] Ao M.,Handbook of Remote Biometrics,2009
- [Coelho and Valença,2010] Coelho E.,Valença J.,A Videovigilância e outros tratamentos de imagem (Dados Pessoais),2010
- [Robert.at al,2000] Robert T.,Introduction to the special section on video surveillance ,IEEE Trans. on Pattern Analysis and Machine Intelligence (PAMI),2000
- [Faux.at al,1985] Faux F.,Theory of evidence for face detection and tracking,2012.
- [Gould and Lewis] Gould J.,Lewis C., Designing for Usability: Key Principles and What Designers Think, Communications of the ACM ,1985
- [Groza.at.al,2009] Groza B.,Towards Developing Secure Video Surveillance Systems over IP, Internet Monitoring and Protection, 2009. ICIMP '09. Fourth International Conference on,2009
- [Lovell.at al,2008] Lovell B.,Real-time Face Detection and Classification for ICCTV Real-time Face Detection and Classification for ICCTV,2008
- [Ahmad,2008] Ahmad I.,Special issue on video surveillance, IEEE Transactions on Circuits and Systems for Video Technology, 2008
- [Appiah.at al,2009] Appiah K.,Autonomous real-time surveillance system with distributed IP cameras,2009
- [AXIS Communication] Vigilância através de câmeras térmicas,2010
- [Boonma.at al,2011] Boonma N.,Image recorder server with IP camera and pocket PC, Procedia Engineering, 2011
- [Brey,2004] Brey.P,Ethical aspects of facial recognition systems in public places, Journal of Information, Communication and Ethics in Society,2004
- [Dalvi.at al,2015] Dalvi R.,Motion Detection & Video Surveillance System using Ip Camera, www.ijaict.com,2015.
- [Duque.at al,2007] Duque D.,Prediction of Abnormal Behaviors for Intelligent Video Surveillance Systems, 2007
- [Ponte] Ponte P.,Projeto de uma Câmara em Rede em FPGA,2013
- [Hintermaier and Wolfgang Steinbach,2010] Hintermaier W., Steinbach E.,A system architecture for IP-camera based driver assistance applications, IEEE Intelligent Vehicles Symposium, Proceedings, 2010
- [Lobato,2007] Lobato J.,Compressão de Imagens em Sistemas de Videovigilância,2009.
- [Loureiro,2009] Loureiro E.,Aplicando a usabilidade em projetos *Web*,2008
- [Milani,2007] Milani A.,MySQL - Guia do Programador,2007
- [NIELSEN,1993] NIELSEN J.,Usability Engineering. Boston: Academic Press, 1993
- [Oliva,2012] Oliva D.,Paradigmas da vigilância – desenvolvimentos tecnológicos da imagem e da segurança,2012
- [Oliveira,2007] Oliveira J.,A formação da segurança privada,2007
- [Paper, White] MJPEG vs MPEG4, www.onssi.com
- [Paper, White] Whitepaper IP Networking and Its Impact on Video Surveillance
- [Peixoto,2012] Peixoto P.,Detecção e acompanhamento de movement através de uma câmara video,2012

- [Pinho,2010] Pinho M.,Detecção e seguimento automáticos de faces humanas em vídeos capturados em ambientes não controlados,2010
- [Prata, Paula] Prata P.,
http://www.di.ubi.pt/~pprata/fsi/FSI_06_07_T1.pdf,2007.
- [Preece.at al,2005] Preece J.,SHARP, Helen. Design de interação: além da interação homem-computador. Porto Alegre: Bookman, 2005
- [Prior,2011] Prior H.,Democracia deliberativa e vigilância electrónica: da participação ao panóptico cibernético,2011
- [Rashmi.at al,2013] Video Surveillance System And Facility To Access Pc From Remote Areas Using Smart Phone,2013
- [Rubin,1994] Rubin J.,Handbook of Usability Testing: How to Plan, Design and Conduct Effective Tests. New York: John Wiley & Sons, Inc., 1994
- [Viana, 2010] Viana J.Mestrado em Ciências Militares Especialidade de Segurança (GNR),2010
- [Zhuang and Wang,2006] Zhuang H., Wang Z.,IP-based real time video monitoring system with controllable platform,2006
- Decreto-Lei 207/ 2005 <http://www.cnpd.pt/bin/legis/nacional/DL207-2005-RADARES.pdf>
- Lei 1/ 2005 http://www.apav.pt/apav_v3/images/pdf/camaras_video.pdf
- Lei 34/ 2013 http://www.psp.pt/SP_Legislacao/Lei%20n.%C2%BA%2034-2013,%20de%2016%20de%20Maio.pdf

6 Anexos

6.1 Anexo 1 -Mockup da primeira versão da página Web

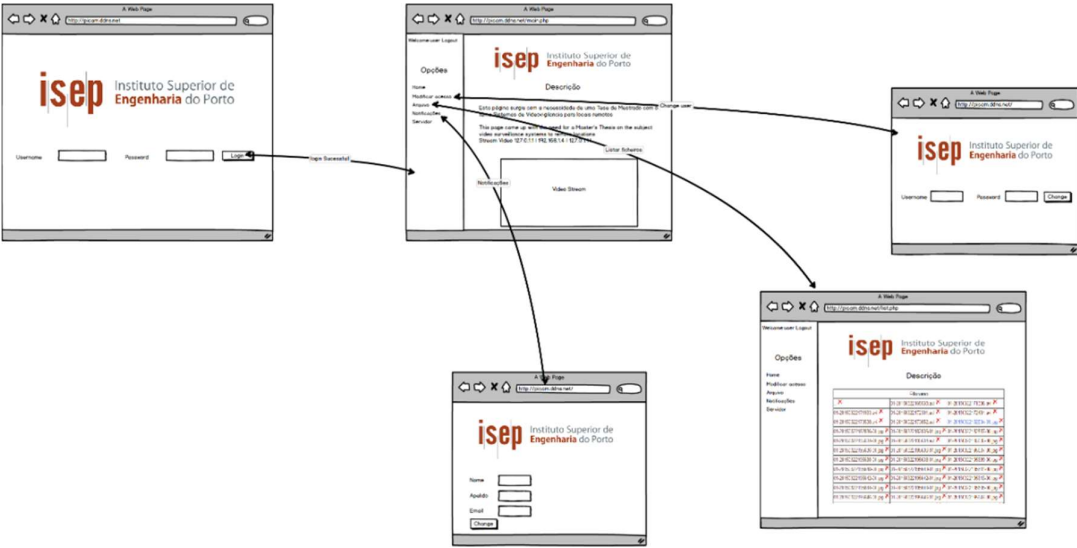


Figura 79 Mockup da página Web

6.2 Anexo 2 - Mockup da segunda versão da página Web



Figura 80 Mockup 2 versão página Web

6.3 Anexo 3 - Questionário de avaliação do protótipo

Questionário e avaliação do protótipo de videovigilância(SVR)

Respondido online no endereço:

<http://goo.gl/forms/bGlpwNXcJm>

Avaliação do sistema de videovigilância SVR

*Obrigatório

Qual o seu sexo? *

☐ Masculino

☐ Feminino

Qual a sua idade? *

☐ Menos de 18

☐ 19 a 25

☐ 26 a 35

☐ 36 a 45

☐ Mais de 56

Qual a sua habilitação literária?

☐ 9ºAno

☐ 12ºAno

☐ Bacharelato

☐ Licenciatura

☐ Mestrado

☐ Doutorado

☐ Outra:

Já teve contacto com algum sistema de videovigilância?

- ☐ Sim
- ☐ Não

Acha que os sistemas de videovigilância têm utilidade?

- ☐ Sim
- ☐ Não

Um sistema de videovigilância para locais remotos sem energia eléctrica seria útil?

- ☐ Sim
- ☐ Não

Adquiriria um sistema de videovigilância para locais remotos?

- ☐ Sim
- ☐ Não

Acha importante a camuflagem de sistemas de videovigilância?

- ☐ Sim
- ☐ Não

Qual a sua opinião em relação ao camuflado do sistema SVR?

- ☐ Mau
- ☐ Não satisfatório
- ☐ Satisfatório
- ☐ Bom
- ☐ Excelente

Acha que a montagem e colocação em funcionamento do sistema de videovigilância SVR é simples?

- ☒ Sim
☐ Não

Classifique a usabilidade do sistema de videovigilância remota (SVR)

1 2 3 4 5

Pouco Satisfatória ☐ ☐ ☐ ☐ ☒ Excelente

Como classifica o sistema SVR na sua inovação?

1 2 3 4 5

Pouco inovador ☐ ☐ ☐ ☐ ☒ Bastante inovador

Como classifica o sistema SVR em relação à qualidade de imagem?

1 2 3 4 5

Qualidade fraca ☐ ☐ ☐ ☐ ☒ Qualidade excelente

Classifique o algoritmo de intrusão do SVR

1 2 3 4 5

Pouco satisfatório ☐ ☐ ☐ ☐ ☒ Excelente

6.4 Anexo 4 - Opções do servidor de stream

Tabela com as diferentes opções disponíveis no servidor.

Option	Range/Values Default	Description
area_detect	Values: 1 - 999999999 Default: Not defined	Detect motion center in predefined areas. A script (on_area_detected) is started immediately when motion center is detected in one of the given areas, but only once during an event even if there is motion in a different configured area.
auto_brightness	Values: on, off Default: off	Let motion regulate the brightness of a video device. Only recommended for cameras without auto brightness
brightness	Values: 0 - 255 Default: 0 (disabled)	The brightness level for the video device.
contrast	Values: 0 - 255 Default: 0 (disabled)	The contrast level for the video device.
control_authentication	Values: Max 4096 characters Default: Not defined	To protect HTTP Control by username and password, use this option for HTTP 1.1 Basic authentication. The string is specified as username:password. Do not specify this option for no authentication. This option must be placed in motion.conf and not in a thread config file.
control_html_output	Values: on, off Default: on	Enable HTML in the answer sent back to a browser connecting to the control_port. This option must be placed in motion.conf and not in a thread config file.
control_localhost	Values: on, off Default: on	Limits the http (html) control to the localhost. This option must be placed in motion.conf and not in a thread config file.
control_port	Values: 0 - 65535 Default: 0 (disabled)	Sets the port number for the http (html using browser) based remote control. This option must be placed in motion.conf and not in a thread config file.
daemon	Values: on, off Default: off	Start in daemon (background) mode and release terminal. This option must be placed in motion.conf and not in a thread config file.

despeckle	Values: EedDI Default: Not defined	Despeckle motion image using combinations of (E/e)rode or (D/d)ilate. And ending with optional (l)abeling.
ffmpeg_bps	Values: 0 - 9999999 Default: 400000	Bitrate of mpegs produced by ffmpeg. Bitrate is bits per second. Default: 400000 (400kbps). Higher value mans better quality and larger files. Option requires that ffmpeg libraries are installed.
ffmpeg_cap_motion	Values: on, off Default: off	Use ffmpeg libraries to encode motion type mpeg movies where you only see the pixels that changes.
ffmpeg_cap_new	Values: on, off Default: off	Use ffmpeg libraries to encode mpeg movies in realtime.
ffmpeg_deinterlace	Values: on, off Default: off	Use ffmpeg to deinterlace video. Necessary if you use an analog camera and see horizontal combing on moving objects in video or pictures.
ffmpeg_filename (now called movie_filename)	Values: Max 4095 characters Default: %v-%Y%m%d%H%M%S	File path for motion triggered ffmpeg movies (mpeg) relative to target_dir. This option was renamed to movie_filename in 3.2.5 to enable better integration of alternative movie libraries to the current ffmpeg solution.
ffmpeg_timelapse	Values: 0 - 2147483647 Default: 0 (disabled)	Create a timelapse movie saving a picture frame at the interval in seconds set by this parameter. Set it to 0 if not used.
ffmpeg_timelapse_mode	Values: hourly, daily, weekly-sunday, weekly-monday, monthly, manual Default: daily	The file rollover mode of the timelapse video.
ffmpeg_variable_bitrate	Values: 0, 2 - 31 Default: 0 (disabled)	Enables and defines variable bitrate for the ffmpeg encoder. ffmpeg_bps is ignored if variable bitrate is enabled. Valid values: 0 (default) = fixed bitrate defined by ffmpeg_bps, or the range 2 - 31 where 2 means best quality and 31 is worst.
ffmpeg_video_codec	Values: mpeg1 (ffmpeg-0.4.8 only), mpeg4, msmpeg4, swf, flv, ffv1, mov Default: mpeg4	Codec to be used by ffmpeg for the video compression. Timelapse mpegs are always made in mpeg1 format independent from this option.
framerate	Values: 2 - 100 Default: 100 (no limit)	Maximum number of frames to be captured from the camera per second.

frequency	Values: 0 - 999999 Default: 0 (Not set)	The frequency to set the tuner to (kHz). Valid range: per tuner spec, default: 0 (Don't set it)
gap	Values: 0 - 2147483647 Default: 60	Gap is the seconds of no motion detection that triggers the end of an event. An event is defined as a series of motion images taken within a short timeframe.
height	Values: Device Dependent Default: 288	The height of each frame in pixels.
hue	Values: 0 - 255 Default: 0 (disabled)	The hue level for the video device.
input	Values: 0 - 7, 8 = disabled Default: 8 (disabled)	Input channel to use expressed as an integer number starting from 0. Should normally be set to 1 for video/TV cards, and 8 for USB cameras.
jpeg_filename	Values: Max 4095 characters Default: %v-%Y%m%d%H%M%S-%q	File path for motion triggered images (jpeg or ppm) relative to target_dir. Value 'preview' makes a jpeg filename with the same name body as the associated saved mpeg movie file.
lightswitch	Values: 0 - 100 Default: 0 (disabled)	Ignore sudden massive light intensity changes given as a percentage of the picture area that changed intensity.
locate	Values: on, off, preview Default: off	Locate and draw a box around the moving object. Value 'preview' makes Motion only draw a box on a saved preview jpeg image and not on the saved mpeg movie.
mask_file	Values: Max 4095 characters Default: Not defined	PGM file to use as a sensitivity mask. This picture MUST have the same width and height as the frames being captured and be in binary format.
max_mpeg_time	Values: 0 (infinite) - 2147483647 Default: 3600	The maximum length of an mpeg movie in seconds. Set this to zero for unlimited length.
minimum_frame_time	Values: 0 - 2147483647 Default: 0	Minimum time in seconds between the capturing picture frames from the camera. Default: 0 = disabled - the capture rate is given by the camera framerate.
minimum_motion_frames	Values: 1 - 1000s Default: 1	Picture frames must contain motion at least the specified number of frames in a row before they are detected as true motion. At the default of 1,

		all motion is detected. Valid range is 1 to thousands, but it is recommended to keep it within 1-5.
motion_video_pipe	Values: Max 4095 characters Default: Not defined	The video4linux video loopback input device for motion images. If a particular pipe is to be used then use the device filename of this pipe, if a dash '-' is given motion will use /proc/video/vloopback/vloopbacks to locate a free pipe. Default: not set
movie_filename	Values: Max 4095 characters Default: %v-%Y%m%d%H%M%S	File path for motion triggered ffmpeg movies (mpeg) relative to target_dir. This was previously called ffmpeg_filename.
mysql_db	Values: Max 4095 characters Default: Not defined	Name of the MySQL database.
mysql_host	Values: Max 4095 characters Default: localhost	IP address or domain name for the MySQL server. Use "localhost" if motion and MySQL runs on the same server.
mysql_password	Values: Max 4095 characters Default: Not defined	The MySQL password.
mysql_user	Values: Max 4095 characters Default: Not defined	The MySQL user name.
netcam_http	Values: 1.0, keep_alive, 1.1 Default: 1.0	The setting for keep-alive of network socket, should improve performance on compatible net cameras. (new in 3.2.10)
netcam_proxy	Values: Max 4095 characters Default: Not defined	URL to use for a netcam proxy server, if required. The syntax is http://myproxy:portnumber
netcam_tolerant_check	Values: on, off Default: off	Set less strict jpeg checks for network cameras with a poor/buggy firmware.
netcam_url	Values: Max 4095 characters Default: Not defined	Specify an url to a downloadable jpeg file or raw mjpeg stream to use as input device. Such as an AXIS 2100 network camera.
netcam_userpass	Values: Max 4095 characters Default: Not defined	For network cameras protected by username and password, use this option for HTTP 1.1 Basic authentication. The string is specified as username:password. Do not specify this option for no authentication.
noise_level	Values: 1 - 255 Default: 32	The noise level is used as a threshold for distinguishing between noise and motion.

noise_tune	Values: on, off Default: on	Activates the automatic tuning of noise level.
norm	Values: 0 (PAL), 1 (NTSC), 2 (SECAM), 3 (PAL NC no colour) Default: 0 (PAL)	Select the norm of the video device. Values: 0 (PAL), 1 (NTSC), 2 (SECAM), 3 (PAL NC no colour). Default: 0 (PAL)
on_area_detected	Values: Max 4095 characters Default: Not defined	Command to be executed when motion in a predefined area is detected. Check option area_detect.
on_camera_lost	Values: Max 4095 characters Default: Not defined	Command to be executed when a camera can't be opened or if it is lost. You can use Conversion Specifiers and spaces as part of the command. Use %f for passing filename (with full path) to the command. (new in 3.2.10)
on_event_end	Values: Max 4095 characters Default: Not defined	Command to be executed when an event ends after a period of no motion. The period of no motion is defined by option gap. You can use Conversion Specifiers and spaces as part of the command.
on_event_start	Values: Max 4095 characters Default: Not defined	Command to be executed when an event starts. An event starts at first motion detected after a period of no motion defined by gap. You can use Conversion Specifiers and spaces as part of the command.
on_motion_detected	Values: Max 4095 characters Default: Not defined	Command to be executed when a motion frame is detected. You can use Conversion Specifiers and spaces as part of the command.
on_movie_end	Values: Max 4095 characters Default: Not defined	Command to be executed when an ffmpeg movie is closed at the end of an event. You can use Conversion Specifiers and spaces as part of the command. Use %f for passing filename (with full path) to the command.
on_movie_start	Values: Max 4095 characters Default: Not defined	Command to be executed when an mpeg movie is created. You can use Conversion Specifiers and spaces as part of the command. Use %f for passing filename (with full path) to the command.
on_picture_save	Values: Max 4095 characters Default: Not defined	Command to be executed when an image is saved. You can use Conversion Specifiers and

		spaces as part of the command. Use %f for passing filename (with full path) to the command.
output_all	Values: on, off Default: off	Picture are saved continuously as if motion was detected all the time.
output_motion	Values: on, off Default: off	Output pictures with only the moving object. This feature generates the special motion type movies where you only see the pixels that changes as a graytone image. If labelling is enabled you see the largest area in blue. Smartmask is shown in red.
output_normal	Values: on, off, first, best, center (since 3.2.10) Default: on	Normal image is an image that is stored when motion is detected. It is the same image that was taken by the camera. I.e. not a motion image like defined by output_motion. Default is that normal images are stored.
pgsql_db	Values: Max 4095 characters Default: Not defined	Name of the PostgreSQL database.
pgsql_host	Values: Max 4095 characters Default: localhost	IP address or domain name for the PostgreSQL server. Use "localhost" if motion and PostgreSQL runs on the same server.
pgsql_password	Values: Max 4095 characters Default: Not defined	The PostgreSQL password.
pgsql_port	Values: 0 - 65535 Default: 5432	The PostgreSQL server port number.
pgsql_user	Values: Max 4095 characters Default: Not defined	The PostgreSQL user name.
post_capture	Values: 0 - 2147483647 Default: 0 (disabled)	Specifies the number of frames to be captured after motion has been detected.
ppm	Values: on, off Default: off	Output ppm images instead of jpeg. This uses less CPU time, but causes a LOT of hard disk I/O, and it is generally slower than jpeg.
pre_capture	Values: 0 - 100s Default: 0 (disabled)	Specifies the number of previous frames to be outputted at motion detection. Recommended range: 0 to 5, default=0. Do not use large values! Large values will cause Motion to skip video frames and cause unsmooth mpegs. To smooth mpegs use larger values of post_capture instead.

process_id_file	Values: Max 4095 characters Default: Not defined	File to store the process ID, also called pid file. Recommended value when used: /var/run/motion.pid
quality	Values: 1 - 100 Default: 75	The quality for the jpeg images in percent.
quiet	Values: on, off Default: off	Be quiet, don't output beeps when detecting motion.
rotate	Values: 0, 90, 180, 270 Default: 0 (not rotated)	Rotate image the given number of degrees. The rotation affects all saved images as well as mpeg movies.
roundrobin_frames	Values: 1 - 2147483647 Default: 1	Specifies the number of frames to capture before switching inputs, this way also slow switching (e.g. every second) is possible.
roundrobin_skip	Values: 1 - 2147483647 Default: 1	Specifies the number of frames to skip after a switch. (1 if you are feeling lucky, 2 if you want to be safe).
saturation	Values: 0 - 255 Default: 0 (disabled)	The colour saturation level for the video device.
setup_mode	Values: on, off Default: off	Run Motion in setup mode.
smart_mask_speed	Values: 0 - 10 Default: 0 (disabled)	Slugginess of the smart mask. Default is 0 = DISABLED. 1 is slow, 10 is fast.
snapshot_filename	Values: Max 4095 characters Default: %v-%Y%m%d%H%M%S-snapshot	File path for snapshots (jpeg or ppm) relative to target_dir.
snapshot_interval	Values: 0 - 2147483647 Default: 0 (disabled)	Make automated snapshots every 'snapshot_interval' seconds.
sql_log_image	Values: on, off Default: on	Log to the database when creating motion triggered image file.
sql_log_mpeg	Values: on, off Default: off	Log to the database when creating motion triggered mpeg file.
sql_log_snapshot	Values: on, off Default: on	Log to the database when creating a snapshot image file.
sql_log_timelapse	Values: on, off Default: off	Log to the database when creating timelapse mpeg file

sql_query	Values: Max 4095 characters Default: insert into security(camera, filename, frame, file_type, time_stamp, text_event) values('%t', '%f', '%q', '%n', '%Y-%m-%d %T', '%C')	SQL query string that is sent to the database. The values for each field are given by using conversion specifiers
switchfilter	Values: on, off Default: off	Turns the switch filter on or off. The filter can distinguish between most switching noise and real motion. With this you can even set roundrobin_skip to 1 without generating much false detection.
target_dir	Values: Max 4095 characters Default: Not defined = current working directory	Target directory for picture and movie files.
text_changes	Values: on, off Default: off	Turns the text showing changed pixels on/off.
text_double	Values: on, off Default: off	Draw characters at twice normal size on images.
text_event	Values: Max 4095 characters Default: %Y%m%d%H%M%S	This option defines the value of the special event conversion specifier %C. You can use any conversion specifier in this option except %C. Date and time values are from the timestamp of the first image in the current event.
text_left	Values: Max 4095 characters Default: Not defined	User defined text overlayed on each in the lower left corner. Use A-Z, a-z, 0-9, " / () @ ~ # < > , . : - + _ \n and vertical bar and conversion specifiers (codes starting by a %).
text_right	Values: Max 4095 characters Default: %Y-%m-%d\n%T	User defined text overlayed on each in the lower right corner. Use A-Z, a-z, 0-9, " / () @ ~ # < > , . : - + _ \n and vertical bar and conversion specifiers (codes starting by a %). Default: %Y-%m-%d\n%T = date in ISO format and time in 24 hour clock
thread	Values: Max 4095 characters Default: Not defined	Specifies full path and filename for a thread config file. Each camera needs a thread config file containing the options that are unique to the camera. If you only have one camera you do not

		need thread config files. If you have two or more cameras you need one thread config file for each camera in addition to motion.conf. This option must be placed in motion.conf and not in a thread config file.
threshold	Values: 1 - 2147483647 Default: 1500	Threshold for declaring motion. The threshold is the number of changed pixels counted after noise filtering, masking, despeckle, and labelling.
threshold_tune	Values: on, off Default: off	Activates the automatic tuning of threshold level. (It's broken)
timelapse_filename	Values: Max 4095 characters Default: %v-%Y%m%d-timelapse	File path for timelapse mpegs relative to target_dir (ffmpeg only).
track_auto	Values: on, off Default: off	Enable auto tracking
track_iomojo_id	Values: 0 - 65535 Default: 0	Use this option if you have an iomojo smilecam connected to the serial port instead of a general stepper motor controller.
track_maxx	Values: 0 - 65535 Default: 0	The maximum position for servo x.
track_maxy	Values: 0 - 65535 Default: 0	The maximum position for servo y.
track_motorx	Values: 0 - 65535 Default: 0	The motor number that is used for controlling the x-axis.
track_motory	Values: 0 - 65535 Default: 0	The motor number that is used for controlling the y-axis.
track_move_wait	Values: 0 - 65535 Default: 10	Delay during which tracking is disabled after auto tracking has moved the camera. Delay is defined as number of picture frames.
track_port	Values: Max 4095 characters Default: Not defined	This is the device name of the serial port to which the stepper motor interface is connected.
track_speed	Values: 0 - 255 Default: 255	Speed to set the motor to.
track_step_angle_x	Values: 0-90 Default: 10	Angle in degrees the camera moves per step on the X-axis with auto tracking. Currently only used with pwc type cameras.

track_step_angle_y	Values: 0-40 Default: 10	Angle in degrees the camera moves per step on the Y-axis with auto tracking. Currently only used with pwc type cameras.
track_stepsize	Values: 0 - 255 Default: 40	Number of steps to make.
track_type	Values: 0 (none), 1 (stepper), 2 (iomojo), 3 (pwc), 4 (generic), 5 (uvcvideo) Default: 0 (None)	Type of tracker.
tunerdevice	Values: Max 4095 characters Default: /dev/tuner0	The tuner device used for controlling the tuner in a tuner card. This option is only used when Motion is compiled for <u>FreeBSD</u> .
v4l2_palette	Values: 0 - 8 Default: 8	Allow to choose preferable palette to be use by motion to capture from those supported by your videodevice. (new in 3.2.10)
video_pipe	Values: Max 4095 characters Default: Not defined	The video4linux video loopback input device for normal images. If a particular pipe is to be used then use the device filename of this pipe. If a dash '-' is given motion will use /proc/video/vloopback/vloopbacks to locate a free pipe.
videodevice	Values: Max 4095 characters Default: /dev/video0 (FreeBSD: /dev/bktr0)	The video device to be used for capturing. Default for Linux is /dev/video0. for <u>FreeBSD</u> the default is /dev/bktr0.
Webcam_limit	Values: 0 - 2147483647 Default: 0 (unlimited)	Limit the number of frames to number frames. After 'Webcam_limit' number of frames the connection will be closed by motion. The value 0 means unlimited.
Webcam_localhost	Values: on, off Default: on	Limits the access to the Webcam to the localhost.
Webcam_maxrate	Values: 1 - 100 Default: 1	Limit the framerate of the Webcam in frames per second. Default is 1. Set the value to 100 for practically unlimited.
Webcam_motion	Values: on, off Default: off	If set to 'on' Motion sends slows down the Webcam stream to 1 picture per second when no motion is detected. When motion is detected the stream runs as defined by Webcam_maxrate.

		When 'off' the <i>Webcam</i> stream always runs as defined by <i>Webcam_maxrate</i> .
<i>Webcam_port</i>	Values: 0 - 65535 Default: 0 (disabled)	TCP port on which motion will listen for incoming connects with its <i>Webcam</i> server.
<i>Webcam_quality</i>	Values: 1 - 100 Default: 50	Quality setting in percent for the mjpeg picture frames transferred over the <i>Webcam</i> connection. Keep it low to restrict needed bandwidth.
width	Values: Device Dependent Default: 352	The width in pixels of each frame. Valid range is camera dependent.

Tabela 5 Tabela de todas as opções do Servidor Motion

6.5 Anexo 5 - Especificadores de texto aceites pelo servidor

Conversion Specifier	Description
%a	The abbreviated weekday name according to the current locale.
%A	The full weekday name according to the current locale.
%b	The abbreviated month name according to the current locale.
%B	The full month name according to the current locale.
%c	The preferred date and time representation for the current locale.
%C	Text defined by the text_event feature
%d	The day of the month as a decimal number (range 01 to 31).
%D	Number of pixels detected as Motion. If labelling is enabled the number is the number of pixels in the largest labelled motion area.
%E	Modifier: use alternative format, see below.
%f	File name - used in the on_picture_save, on_movie_start, on_movie_end, and sql_query features.
%F	Equivalent to %Y-%m-%d (the ISO 8601 date format).
%H	The hour as a decimal number using a 24-hour clock (range 00 to 23).
%i	Width of the rectangle containing the motion pixels (the rectangle that is shown on the image when locate is on).
%I	The hour as a decimal number using a 12-hour clock (range 01 to 12).
%j	The day of the year as a decimal number (range 001 to 366).
%J	Height of the rectangle containing the motion pixels (the rectangle that is shown on the image when locate is on).
%k	The hour (24-hour clock) as a decimal number (range 0 to 23); single digits are preceded by a blank. (See also %H.)
%K	X coordinate in pixels of the center point of motion. Origin is upper left corner.
%l	The hour (12-hour clock) as a decimal number (range 1 to 12); single digits are preceded by a blank. (See also %I.)
%L	Y coordinate in pixels of the center point of motion. Origin is upper left corner and number is positive moving downwards (I may change this soon).
%m	The month as a decimal number (range 01 to 12).
%M	The minute as a decimal number (range 00 to 59).

%n	Filetype as used in the on_picture_save, on_movie_start, on_movie_end, and sql_query features.
%N	Noise level.
%o	Threshold. The number of detected pixels required to trigger motion. When threshold_tune is 'on' this can be used to show the current tuned value of threshold.
%p	Either 'AM' or 'PM' according to the given time value, or the corresponding strings for the current locale. Noon is treated as `pm' and midnight as `am'.
%P	Like %p but in lowercase: `am' or `pm' or a corresponding string for the current locale.
%q	Picture frame number within current second. For jpeg filenames this should always be included in the filename if you save more than 1 picture per second to ensure unique filenames. It is not needed in filenames for mpegs.
%Q	Number of detected labels found by the despeckle feature
%r	The time in a.m. or p.m. notation.
%R	The time in 24-hour notation (%H:%M).
%s	The number of seconds since the Epoch, i.e., since 1970-01-01 00:00:00 UTC.
%S	The second as a decimal number (range 00 to 61).
%t	Thread number (camera number)
%T	The time in 24-hour notation (%H:%M:%S).
%u	The day of the week as a decimal, range 1 to 7, Monday being 1. See also %w.
%U	The week number of the current year as a decimal number, range 00 to 53, starting with the first Sunday as the first day of week 01. See also %V and %W.
%v	Event number. An event is a series of motion detections happening with less than 'gap' seconds between them.
%V	The ISO 8601:1988 week number of the current year as a decimal number, range 01 to 53, where week 1 is the first week that has at least 4 days in the current year, and with Monday as the first day of the week. See also %U and %W.
%w	The day of the week as a decimal, range 0 to 6, Sunday being 0. See also %u.
%W	The week number of the current year as a decimal number, range 00 to 53, starting with the first Monday as the first day of week 01.

%x	The preferred date representation for the current locale without the time.
%X	The preferred time representation for the current locale without the date.
%y	The year as a decimal number without a century (range 00 to 99).
%Y	The year as a decimal number including the century.
%z	The time-zone as hour offset from GMT.
%Z	The time zone or name or abbreviation.

Tabela 6 Tabela de todos especificadores de texto aceites pelo Servidor Motion